THÈSE DE DROIT PUBLIC

Droit du Cyberespace : Technologies et innovations numériques

Pour obtenir le grade de Docteur de l'Université de Lille

Présentée par

Laurène BAUDOUIN

Sûreté et sécurité au XXI^{ème} siècle

L'exemple des drones aériens « augmentés » de sécurité publique

JURY

Directeur de thèse : Monsieur Marcel MORITZ, MCF-HDR de droit public, Université de Lille

Membres du jury :

Monsieur Stéphane BRACQ, Professeur de droit public, Sciences Po Lille (Président du jury)

Monsieur Xavier DUPRÉ DE BOULOIS, Professeur de droit public, Université de Panthéon-Sorbonne (Rapporteur)

Monsieur Fouad EDDAZI, Maître de conférences en droit public, Université d'Orléans

Monsieur Xavier LATOUR, Professeur de droit public, Université de Côte d'Azur (Rapporteur)

Date de soutenance : 21 mars 2024

SÛRETÉ ET SÉCURITÉ AU XXI^{ème} SIÈCLE

L'EXEMPLE DES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

À la mémoire de mon papa,

À ma maman,

À la mémoire de mes grands-parents,

À ma grand-mère,

À mes amis,

À la mémoire d'Acaa.

REMERCIEMENTS

Tout d'abord, je tiens à exprimer ma reconnaissance à mon directeur de thèse, Monsieur Marcel Moritz, Avocat et Maître de conférences-HDR de droit public à l'Université de Lille, pour sa pédagogie, ses conseils et ses encouragements tout au long de l'élaboration de cette étude. Je remercie également Monsieur Stéphane Bracq, Professeur de droit public à Sciences Po Lille, ainsi que Madame Noémie Véron, Maîtresse de conférences en droit public, pour la richesse de leurs réflexions et pour leurs conseils avisés en matière méthodologique.

Je souhaite, ensuite, remercier chaleureusement mon collègue Hugo Lami, doctorant en droit public, et Romane Delepoulle, étudiante en Master de droit du numérique, pour leur relecture attentive, ainsi qu'Audrey, Luis, Román, Sébastien et Tilila pour leur soutien. Un grand merci aussi à mes amis de France et de Belgique pour leurs encouragements.

Je tiens aussi à exprimer toute ma gratitude envers le laboratoire du CERAPS de l'Université de Lille qui m'a offert l'opportunité d'écrire cette thèse et de développer ma réflexion juridique mais également pour avoir partagé leurs connaissances des enjeux politiques et sociologiques dans le cadre des travaux de recherche des projets sur lesquels nous avons travaillé. Je remercie également les partenaires des projets COOPOL, S2UCRE et GIRAFE pour leurs contributions.

Enfin, un immense merci à mes parents pour leurs conseils, leur assistance à la relecture et leur soutien indéfectible au cours de mes années de thèse et sans qui elle ne serait pas arrivée au bout.

LISTE DES PRINCIPALES ABRÉVIATIONS

AAI	Autorités administratives indépendantes
act.	actualité
AESA/*EASA*	Agence Européenne de la Sécurité Aérienne/ *European Union Aviation Safety Agency*
aff.	affaire
AJDA	*Actualités juridiques - Droit administratif* (Dalloz)
AJP	*Actualités juridiques pénales* (Dalloz)
AN	Assemblée nationale
ANSSI	Assemblée Nationale de la Sécurité des Systèmes Informatiques
art.	article
c.	contre
CA	Cour d'appel
CAA	Cour administrative d'appel
CAC	Code de l'aviation civile
CAHAI	Comité *Ad Hoc* sur l'Intelligence artificielle du Conseil de l'Europe
C. cass.	Cour de cassation
C. civ.	Code civil
C. const.	Conseil constitutionnel
CDFUE	Charte des droits fondamentaux de l'Union européenne
CE	Conseil d'État
CE, ass.	Assemblée du contentieux du Conseil d'État
CE, ord.	Ordonnance de référé du Conseil d'État
CEDH	Cour européenne des droits de l'Homme
CEIA	Comité européen de l'Intelligence artificielle
cf.	Référence
CGCT	Code général des collectivités territoriales
CHEMI	Centre des Hautes Études du Ministère de l'Intérieur
ch. crim.	chambre criminelle
chron.	chronique
CJA	Code de justice administrative

CJCE	Cour de Justice des Communautés européennes
CJUE	Cour de justice de l'Union européenne
CNCDH	Commission nationale consultative des droits de l'Homme
CNIL	Commission nationale informatique et libertés
coll.	collection
comm.	commentaire
cons.	considérant
Conv. EDH	Convention européenne des droits de l'Homme
CP	Code pénal
CPC	Code de procédure civile
CPCE	Code des postes et des communications électroniques
CPP	Code de procédure pénale
CRPA	Code des relations entre le public et l'administration
CSI	Code de la sécurité intérieure
DA	*Droit administratif*
DACP	Données à caractère personnel
DC	Décision de Conformité du Conseil constitutionnel
DDD	Défenseur des droits
DDHC	Déclaration des droits de l'Homme et du citoyen
DDoS	Attaque par déni de service
DGAC	Direction générale de l'aviation civile
DGSI	Direction générale de la Sécurité intérieure
dir.	Sous la direction de
DPD/*DPO*	Délégué à la Protection des Données/*Data Protection Officier*
DPJ	Directive « Police-Justice » relative à la protection des données dans le domaine pénal
DSAC	Direction de la Sécurité de l'Aviation Civile
DSAÉ	Direction de la sécurité aéronautique d'État
DUDH	Déclaration universelle des droits de l'Homme
***EDPB*/ CEPD**	*European Data Protection Board*/Comité européen de protection des données
***EDPS*/CEPD**	*European Data Protection Supervisor*/Contrôleur européen de la protection des données

et al.	*et alias*/auteurs associés
fasc.	fascicule
Gaz. Pal.	*Gazette du Palais*
GPS	*Global Position System*/Système de Positionnement Global
gr. ch.	grande chambre
IA/*AI*	Intelligence artificielle/*Artificial intelligence*
Idem/Ibid	au même endroit
IHEMI	Institut des hautes études du ministère de l'Intérieur
INHESJ	Institut national des hautes études sur la sécurité et la justice
JCl	*Jurisclasseur LexisNexis*
JCP A	*La Semaine juridique - Administrations et collectivités territoriales*
JCP G	*La Semaine juridique - Édition générale*
JDJ	*Journal du droit des jeunes*
JOP	Jeux Olympiques et Paralympiques
JORF	*Journal officiel de la République Française*
JOUE	*Journal officiel de l'Union européenne*
LGDJ	Librairie générale de droit et de jurisprudence
LIDAR	*Light/Laser Detection and Ranging*
LIL	Loi dite « Informatique et Libertés »
LINC	Laboratoire d'innovation numérique de la CNIL
LOPPSI	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
LOPS	Loi d'orientation et de programmation relative à la sécurité
LOPSI	Loi d'orientation et de programmation pour la sécurité intérieure
LPA	*Les Petites affiches*
n°	numéro
OACI	Organisation de l'Aviation Civile Internationale
obs.	observations
ONU	Organisation des Nations unies
op. cit.	Opus citatum
OTAN	Organisation transatlantique nord
p. pp.	page/pages

PIDCP	Pacte international relatif aux droits civils et politiques
PUAM	Presses universitaires d'Aix-Marseille
PUF	Presses universitaires de France
PULIM	Presses universitaires de Limoges
PUN	Presses universitaires de Nancy
PUR	Presses universitaires de Rennes
QPC	Question prioritaire de constitutionnalité
RDLF	*Revue de Droits et Libertés fondamentaux*
RDP	*Revue de droit public*
Rec.	*Recueil*
REIA	Règlement européen pour l'IA
req.	requête
RFDA	*Revue française de droit administratif*
RGD	*Revue générale du droit*
RGPD	Règlement général sur la protection des données
RLDI	*Revue Lamy de Droit de l'Immatériel*
RPAS	*Remotly Piloted Aircraft System*, système d'aéronef piloté à distance
RPSI	Loi relative à la responsabilité pénale et à la sécurité intérieure
RSC	*Revue de science criminelle et de droit pénal comparé*
RSSI	Responsable des systèmes d'information
SAAD	Système algorithmique d'aide à la prise de décisions
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SI	Systèmes d'information
SIA	Systèmes d'intelligence artificielle
spéc.	spécialement
SSL	*Strategic Subject List*
STAD	Systèmes de Traitement Automatisé de Données
TA	Tribunal administratif
TAJ	Fichier de traitement des antécédents judiciaires
TC	Tribunal des conflits
TGI	Tribunal de Grande Instance
UAS	*Unmanned Air* System/système aérien sans pilote

UAV	*Unmanned Aerial Vehicle*/véhicule aérien sans pilote
UE	Union européenne
vol.	volume
VST	Vie sociale et traitements

SOMMAIRE

INTRODUCTION

1. Ces dernières années, l'introduction de nouvelles technologies occupe une place de choix au cœur de la stratégie de sécurité française. Certaines de ces technologies sont issues du domaine militaire mais bénéficient d'une dualité d'emploi leur permettant des applications directes et indirectes dans le domaine civil[1]. Les drones comptent parmi ces nombreuses innovations technologiques en plein essor, convoités tant par le secteur public que par le secteur privé[2]. D'origine militaire, ils ont vu leur utilisation se généraliser ces deux dernières décennies.

2. Après avoir fait leurs preuves dans le domaine militaire[3], les drones ont investi l'espace aérien national dans le cadre de missions de lutte contre les incendies et de sauvetage[4], dans un premier temps, puis dans de nombreuses autres activités publiques[5] comme civiles[6]. Désormais, ils ont vocation à être utilisés à diverses fins allant des missions de défense à celles visant à répondre

---

[1] DANET (D.), HANON (J-P.) et BOISBOISSEL (G. de) (dir.), *La guerre robotisée*, Paris, éditions Economica, 2012, 336 p., p. 265.

[2] CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, Den Haag, Editor T.M.C Asser Press, Springer, 2016, 386 p. ; Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », 16 novembre 2020, notamment pp. 231-232 [en ligne] ; BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *Dalloz IPT/IT* n°6, 20 juin 2022, pp. 299 et suiv.

[3] Voir notamment : DANET (D.), HANON (J-P.) et BOISBOISSEL (G. de) (dir.), *La guerre robotisée*, *op. cit.* ; CHAMAYOU (G.), *Théorie du drone*, Paris, édition La Fabrique, 2013, 363 p. ; GALLAIS (S.), *Cadre juridique de l'emploi des drones au combat*, Paris, Éditions L'Harmattan, 2013, 191 p. ; MERCIER (D.), *Les drones aériens : passé, présent et avenir. Approche globale*, Paris, La Documentation Française, coll. Stratégie aérospatiale, 2013, 706 p. ; DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, Rennes, PUR, 2015, 267 p. ; EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, Paris, LGDJ, coll. Grands colloques, 2018, 347 p. ; ETCHEVERRY (P.), *Cyber et drones*, Paris, éditions Economica, 2018, 167 p. ; STORR (P.) and STORR (C.), « The Rise and Regulation of Drones : Are We Embracing Minority Report or WALL-E ? », pp. 105-122 *in* CORRALES (M.), FENWICK (M.) and FORGÓ (N.) (Ed.), *Robotics, AI and the Future of Law*, Singapore, Springer, 2018, 237 p. ; Sénat, Rapport d'information n° 559 (2016-2017) « Drones d'observation et drones armés : un enjeu de souveraineté », remis par PERRIN (C.) *et al.*, fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, 23 mai 2017 [en ligne].

[4] DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.* ; RODRIGUEZ (E.), *Drones - Missions de secours de sécurité civile*, Paris, Éditions Carlo Zaglia, coll. Les cahiers du savoir, 2019, 82 p. ; « Incendies : cinq innovations pour lutter contre les feux de forêt », *France Info*, 25 juillet 2017 [en ligne] consulté le 16 juin 2022 ; SERGENT (D.), « Des drones innovants pour lutter contre les feux de forêts », *La Croix*, 6 août 2019 [en ligne] consulté le 16 juin 2022 ; Sapeurs-pompiers de France, « Moyens aériens de la Sécurité civile et des sapeurs-pompiers », [en ligne] consulté le 16 juin 2022 ; SADAUNE (M.), « Utilisation et efficacité professionnelle des drones par les sapeurs-pompiers », pompiers.*fr*, 12 octobre 2017 [en ligne] consulté le 7 juin 2023.

[5] MOREL (J-F.), « Face aux drones, l'approche responsable de la gendarmerie nationale », notamment pp. 260-261 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

[6] HANICOTTE (R.), « Une nouvelle catégorie d'OVNI juridique: les drones », *Gaz. Pal.*, n° 317, 13 novembre 2014, p. 6 ; POURCEL (E.), « Drone aérien : y-a-t-il un pilote « de » l'avion ? », *JCP G*, n°49, 30 novembre 2015, 1312 ; CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.* ; BELLIN (I.) et LABBÉ (S.), *Des Drones à Tout Faire ?: Ce Qu'ils Vont Changer Dans Ma Vie Au Quotidien*, Versailles, Editions Quae, 2016, 203 p. ; BASDEVANT (A.), « La sécurité de l'usage des drones civils aériens », *RLDI* n° 131, 1er novembre 2016, pp. 37-44.

aux exigences de l'ordre public sans oublier leur utilisation dans le cadre d'activités commerciales ou encore de loisirs. Adaptables à de nombreuses situations et à différentes tâches, large sera le panel des activités qui, à l'avenir, auront recours à cet outil aux multiples applications. En outre, ces engins sont conçus pour s'adapter à tout type d'environnement qu'il soit terrestre, maritime ou aérien. Cependant, les drones terrestres et maritimes ne disposent pas d'un développement aussi conséquent que les drones aériens qui suscitent davantage l'intérêt des pouvoirs publics et des sociétés commerciales. Les drones convoités par les forces de sécurité publique sont aussi principalement, voire exclusivement, de type aérien.

3. Depuis déjà plus d'une décennie, les drones aériens sont utilisés par les sapeurs-pompiers dans le cadre de missions de secours hors zone peuplée (en complément d'autres véhicules aériens tels que les avions et hélicoptères d'observation ou bombardiers d'eau, notamment des Canadairs)[7] afin d'enrayer les feux de forêt ou plus généralement les catastrophes naturelles[8]. Les drones aériens n'engendraient alors que peu d'enjeux juridiques. De fait, ils ne survolaient pas d'individus (hormis certains cas exceptionnels) et, par conséquent, ne présentaient pas de risques majeurs pour l'intégrité physique des personnes ou pour l'exercice de leurs droits et libertés[9].

4. Ces dernières années n'ont fait que confirmer la volonté des pouvoirs publics d'introduire les drones aériens de sécurité publique dans l'espace public[10] comme en témoigne le dernier « Livre blanc de la sécurité intérieure »[11] ou encore, de manière plus concrète, leur utilisation par les forces de l'ordre afin d'assurer le respect des règles sanitaires dû au confinement lors de la pandémie de

---

[7] Sapeurs-pompiers de France, « Moyens aériens de la Sécurité civile et des sapeurs-pompiers », *op. cit.*

[8] MASSET (C.), « Gendarmerie du transport aérien : réglementation de l'utilisation des drones aériens », p. 166 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.* ; BELLIN (I.) et LABBÉ (S.), *Des Drones à Tout Faire ? : Ce Qu'ils Vont Changer Dans Ma Vie Au Quotidien*, *op. cit.*, pp. 122-123 ; NORMAND (J-M.), « Les drones, nouvel outil contre les incendies de forêt », *Le Monde*, 12 août 2016 [en ligne] consulté le 16 juin 2022 ; WAWRZYNIAK (R.), « Les nouveaux yeux du secours », *Archives des dossiers du Ministère de l'Intérieur*, 22 janvier 2016 [en ligne] ; HOAREAU (C.), « Drones et lutte contre les feux de forêt : la connectivité, nerf de la guerre », *Journal du Net*, 13 décembre 2021 [en ligne] consulté 16 juin 2022.

[9] Leurs finalités n'étant pas celles d'une collecte de données sur des individus.

[10] À titre d'exemple de la volonté des pouvoirs publics de faire usage de drones aériens à des fins de lutte contre les trafics de marchandises illégales : BERNARD (P.), « Des drones pour sécuriser Marseille, une idée qui séduit », *Le Figaro*, 19 septembre 2013 [en ligne] ; ZAPPI (S.), « À Marseille, des élus PS parlent de drones pour lutter contre le crime », *Le Monde*, 24 septembre 2013 [en ligne] consultés le 12 décembre 2022.

[11] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*

COVID-19[12] en 2020. Les drones aériens ont ainsi fait leur entrée au sein des villes et sont utilisés tant par les services de secours que par les forces de l'ordre[13]. Les gendarmes et les forces de police nationale y avaient notamment déjà eu recours en zone urbaine à des fins de surveillance de manifestations[14]. Cependant, le recours à des drones aériens en milieu urbain à des fins de surveillance implique de nombreux enjeux qui diffèrent sensiblement de ceux engendrés par les drones militaires de défense. Ces enjeux reposent principalement sur leurs capacités à collecter et traiter des données, notamment des données à caractère personnel, que ce soit par l'intermédiaire de caméras ou par d'autres capteurs dont ils peuvent être équipés. Les images enregistrées par une caméra installée sur un drone aérien à l'usage des forces de sécurité publique sont ainsi soumises à la réglementation nationale et européenne relative à la protection des données à caractère personnel (DACP). Cette règlementation se compose de la loi n° 78-17 du 6 janvier 1978[15], dite « Informatique et libertés » (LIL), du règlement européen du 27 avril 2016 relatif à la protection des données à caractère personnel[16] (RGPD) ainsi que de la directive européenne concernant le traitement des données à caractère personnel par les autorités compétentes dans le cadre pénal du 27 avril 2016[17], dite « Police-Justice » (DPJ).

5. Le recours à des moyens issus des technologies de l'information et de la communication (TIC) afin de répondre aux exigences de l'ordre public constitue une solution évidente et s'est

---

[12] LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *Médiapart*, 25 avril 2020 [en ligne] consulté le 27 avril 2020 ; VALDENAIRE (L.), « Drones et hélicoptères : les gendarmes du Grand Est déploient les grands moyens pendant le confinement », *France Bleu*, 10 avril 2020 [en ligne] consulté le 12 décembre 2022.

[13] Voir notamment : MOREL (J-F.) et ABELLARD (M.), « L'emploi des drones, de la gendarmerie au maintien de l'ordre », *Revue de la gendarmerie nationale* n° 267, juin 2020, pp. 121-129 ; CORNEVIN (C.), « Les gendarmes déploient leurs drones », *Le Figaro*, 3 février 2016 [en ligne] ; SIMON (P.), « Notre-Dame-des-Landes, comment les gendarmes ont utilisé des drones », *Ouest France*, 25 juillet 2018 [en ligne] consultés le 12 décembre 2022.

[14] Voir par exemple : « Sécurité routière : les drones policiers ne font pas tomber les PV du ciel », *AFP*, 7 octobre 2016 [en ligne] ; « Euro 2016, la Police renforce sa flotte de drones de surveillance », *Robots & cie*, 10 mai 2016 [en ligne] ; MILLON (L.), « Comment la police française exploite le potentiel des drones », *Siècle digital*, 17 novembre 2017 [en ligne].

[15] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL), *JORF* du 7 janvier 1978 [en ligne] modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0141 du 21 juin 2018 [en ligne].

[16] Règlement (UE) n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données ou RGPD), *JOUE* L 119, 4 mai 2016, pp. 1–88 [en ligne].

[17] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (DPJ), *JOUE* L 119, 4 mai 2016, pp. 89-131 [en ligne].

depuis longtemps systématisé au sein des activités des forces de l'ordre. Parmi les nombreuses avancées technologiques dont elles bénéficient, les algorithmes sont aujourd'hui largement prépondérants, qu'il s'agisse d'analyse d'images issues de caméras de surveillance (ex. détection d'évènements anormaux ou encore d'aide à la recherche d'individus ayant commis une infraction) ou encore de données collectées sur internet à des fins d'enquêtes judiciaires (ex. données issues des réseaux sociaux).

6. Les algorithmes sont devenus des outils incontournables du quotidien pour les individus comme pour les institutions publiques, les gouvernements ou les entreprises[18]. Ils permettent de déléguer différentes tâches à la machine ou peuvent servir d'outil d'aide à la prise de nombreuses décisions. Les algorithmes font ainsi partie intégrante de la société. Aussi, l'introduction de nouvelles générations de procédés algorithmiques entend favoriser l'automatisation de certaines tâches d'analyse ou de prise de décision. Ces développements technologiques en faveur de l'automatisation de tâches plus complexes sont facteurs d'opportunités (économiques ou opérationnels) autant qu'ils suscitent d'enjeux éthiques, juridiques ou de gouvernance[19].

7. L'accroissement du nombre des algorithmes ayant intégré les usages des forces de l'ordre[20] incite à la réflexion, plus particulièrement s'agissant des algorithmes permettant la délégation partielle de tâches d'analyse ou de prise de décision. Le fait est que ces dernières auront potentiellement des conséquences non négligeables pour les personnes concernées[21]. Certes, les

---

[18] De manière non-exhaustive : BASDEVANT (A.) et MIGNARD (J-P.), *L'empire des données - Essai sur la société, les algorithmes et la loi*, Paris, Édition Don Quichotte, 2018, 288 p. ; SADIN (É.), *La vie algorithmique - Critique de la raison numérique*, Paris, Édition L'échappée, coll. « Pour en finir avec », 2015, 288 p. ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022, 360 p., Annexe 9 pp. 267-346 [en ligne].

[19] Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), 28 mars 2018, 235 p. [en ligne] ; Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), vol. I, septembre 2021, 68 p., spéc. pp. 13-23 [en ligne]. Voir aussi : DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, Paris, Éditions Archives contemporaines, 2021, 191 p., p. 6 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, Bruxelles, Bruylant, 2020, 434 p. ; PAPINEAU (C.), « Enjeux éthiques et juridiques des algorithmes au regard des missions de sécurité publique », *Revue de la Gendarmerie Nationale*, 2nd Semestre 2018, pp. 21-25.

[20] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, Paris, L'Harmattan, 2020, 241 p., p. 11 : « Les liens entre la sécurité intérieure et l'IA tendent à se décupler, dans la mesure où cette dernière renforcerait l'efficacité des politiques de sécurité intérieure ».

[21] Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 140 : « il faut adapter la protection des droits et des libertés au regard des abus potentiels liés à l'utilisation des systèmes d'apprentissage machine ».

apports des algorithmes dans le cadre des activités des forces de l'ordre sont nombreux[22] ; pour autant, ces technologies ne sont ni infaillibles ni anodines. Les algorithmes comportent encore de nombreuses limites. Ils peuvent par conséquent être aussi bien porteurs de progrès indispensables à la continuité des activités de sécurité publique que vecteurs d'atteintes aux droits et libertés des personnes[23]. L'étude de leurs usages et de leurs limites fait désormais l'unanimité parmi tous les acteurs y compris les personnes pouvant faire l'objet de leur analyse ou prise de décision[24].

8. Les usages des algorithmes méritent un encadrement adapté à chaque type d'activité ; cadre qui pour l'heure n'a malheureusement pas encore vu le jour. Néanmoins, les institutions européennes ont pris la mesure de l'importance que revêt l'édification d'un cadre unifié en matière d'intelligence artificielle et d'algorithmes. En ce sens, un projet de règlement européen[25] est en cours d'adoption et plusieurs documents annexes[26] ont été publiés en vue de donner une première approche des règles et des recommandations à suivre en matière de développement comme

---

[22] De manière non-exhaustive : LAVENUE (J-J.) et VILLABA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, Villeneuve d'Ascq, Presses universitaires du septentrion, 2011, 294 p. ; Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.* ; Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.* ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, pp. 58-60 ; Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.* ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, spéc. pp. 59-92.

[23] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, Paris, Presses des Mines, 2020, 118 p., p. 47 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, Paris, Dalloz, coll. Le sens du droit - Essai, 2020, 275 p., spéc. pp. 69-80 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, spéc. pp. 15-17.

[24] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*

[25] Commission européenne, « Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle et modifiant certains actes législatifs de l'Union) », 21 avril 2021 [en ligne].

[26] Voir notamment : Commission européenne, « Lignes directrices en matière d'éthique pour l'IA » remises par le GEHN sur IA de la Commission européenne, 8 avril 2019, 41 p. [en ligne] ; Commission européenne, « Livre blanc Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance », 19 février 2020, COM(2020) 65 final, 31 p. [en ligne] ; Comité ministériel du Conseil de l'Europe, « Recommandation aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme », CM/Rec (2020)1, 8 avril 2020, 15 p. [en ligne] ; Parlement européen, « Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes - Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL)) », 20 octobre 2020 [en ligne] ; Parlement européen, « Un régime de responsabilité civile pour l'intelligence artificielle - Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle », 20 octobre 2020 [en ligne] ; Comité *Ad Hoc* sur l'Intelligence artificielle (CAHAI) du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », 17 décembre 2020, 55 p. [disponible en ligne] ; Parlement européen, « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales - Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », 6 octobre 2021 [en ligne].

d'utilisation des algorithmes, suivant le domaine d'activité concerné.

9. L'association de technologies telles que les drones aériens et les algorithmes dans un cadre de sécurité publique suscite de nombreuses interrogations, autant que d'espoirs d'accroissement de l'efficacité des missions[27]. Les propos tenus dans différents médias concernant l'utilisation des drones aériens au sein de l'espace public tendent à susciter l'inquiétude d'une surveillance de masse[28]. Il en va de même s'agissant des outils d'intelligence artificielle et des systèmes algorithmiques dans les domaines régaliens où l'opacité de leurs usages et les exemples étrangers à l'allure de romans dystopiques ne permettent pas d'avoir une vision claire des techniques effectivement mises en œuvre[29].

10. Les drones aériens de sécurité publique, au même titre que les algorithmes utilisés à des fins policières, pâtissent généralement d'une mauvaise réputation[30]. La forte médiatisation de ces technologies, particulièrement s'agissant des outils algorithmiques, ne reflète pas toujours la réalité[31] ; pour autant, les inquiétudes qu'elles suscitent ne doivent pas être mésestimées car elles constituent de véritables enjeux que les informaticiens autant que les juristes s'évertuent à prévenir.

---

[27] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », 19 juillet 2022, 18 p., p. 3 [en ligne] : « La technologie des vidéos dites « augmentées » […] offre de nouvelles perspectives à ses utilisateurs avec une capacité opérationnelle qui tend à s'accroitre au fur et à mesure des avancées réalisées en matière de traitement d'algorithmes dits « d'intelligence artificielle ». Voir aussi : Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, spéc. pp. 13-14.

[28] De manière non-exhaustive : LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *op. cit.* ; « France. La nouvelle loi sur la sécurité globale risque d'instaurer une surveillance d'État démesurée et inacceptable », *Amnesty International*, 3 mars 2021 [en ligne] ; « Sécurité globale : le Sénat dit oui à la surveillance de masse », *La Quadrature du Net*, 19 mars 2021 [en ligne] ; CHAUVIN (H.), « JO 2024 : la France championne de la surveillance de masse », *Reporterre*, 27 janvier 2023 [en ligne] consultés en février 2023.

[29] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, spéc. p. 12 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, spéc. p. 18 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, spéc. pp. 93-113 ; « Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique », *La Quadrature du Net*, 18 janvier 2023 [en ligne] consulté le 18 janvier 2023.

[30] De manière non-exhaustive : Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, spéc. pp. 16-17 : « Une méfiance toute particulière entre en éveil dès lors qu'il s'agit d'utilisation des données par l'État, *a fortiori* dans sa fonction régalienne » ; CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, spec. pp. 47-65 ; CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review Elsevier Ltd*, n°30, 2014, pp. 286-305 ; « Les drones policiers autorisés par le Conseil constitutionnel », *La Quadrature du Net*, 21 janvier 2022 [en ligne] ; ESTIMBRE (T.), « La surveillance de masse par drones policiers devient légale en France », *journal du geek*, 25 janvier 2022 [en ligne] consultés le 30 janvier 2022.

[31] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 69 : « Les prophéties de personnalités médiatiques pour prévenir des dérives de « l'IA » comme le regretté Stephen Hawking ou Elon Musk, ont manqué de saisir les réelles et profondes difficultés posées par cette « IA » composé de neurones formels, en s'égarant dans des spéculations sur une super-intelligence ».

Il importe de garder une vision réaliste et concrète des opportunités et des enjeux qu'engendrent ces technologies. En ce sens, le philosophe et historien Pierre Ducassé avait recensé trois typologies d'attitudes inadéquates face à la technique[32], pouvant s'appliquer aux réactions face aux nouvelles technologies, à savoir : l'antitechnicisme, la technophilie et l'indifférence. Le caractère intrusif de ces technologies de traitement des données questionne l'incidence de leur usage sur les droits individuels. Dans cette volonté de garder un esprit critique, il convient, à l'inverse, de ne pas céder à la tentation d'un rejet systématique sous toutes ses formes et d'analyser ces technologies pour ce qu'elles sont en fonction de leurs actions (capacités techniques) et du contexte dans lequel elles sont utilisées[33].

11. L'introduction des drones aériens de surveillance au sein de l'espace public consiste avant tout à répondre aux besoins des agents dans l'exercice de leurs missions de préservation de l'ordre public. Ces outils entendent pallier les inconvénients que présentent d'autres outils de surveillance (caméras fixes filmant l'espace public, par exemple) et améliorer les performances des activités de police et de secours aux personnes par l'intermédiaire des nombreux progrès technologiques qu'ils comportent. Néanmoins, leur insertion dans l'espace public doit respecter de manière effective un certain nombre de principes issus du droit national et supranational afin de ne pas porter une atteinte disproportionnée aux droits et libertés au motif de vouloir répondre aux exigences de l'ordre public.

12. Les drones aériens associés à des algorithmes d'analyse d'évènements visent à poursuivre les objectifs de renforcement de la sécurité publique réclamés par les autorités publiques. Ils entendent intégrer de manière pérenne les dispositifs à l'usage des forces de l'ordre comme ceux des services de secours. Les drones aériens s'insèrent parfaitement au sein de la politique actuelle en faveur d'une augmentation de la sécurité intérieure qui fait l'objet d'une demande croissante depuis les attentats du 11 septembre 2001 renforcée par ceux perpétrés en France, notamment depuis 2015. La question de la sécurité est toujours prégnante dans les débats politiques généraux et plus spécifiquement au cœur des politiques pénales judiciaires et policières. Dans leur poursuite d'amélioration de la sécurité publique, les drones aériens associés à des algorithmes d'analyse d'évènements viennent s'inscrire au sein de la thématique « sécurité et liberté » et questionnent tant l'existence du droit à la sécurité, voire d'un droit fondamental à la sécurité, que l'adéquation des

---

[32] DUCASSÉ (P.), *Les techniques et le philosophe*, Paris, PUF, 1958, 176 p.

[33] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, pp. 2-3 et 5-6.

garanties servant à préserver les droits et libertés - reconnus comme fondamentaux - auxquels il doit être concilié.

13. L'attrait pour le recours aux algorithmes d'aide à la prise de décision à des fins de sécurité publique résulte des progrès technologiques qui ont pu être constatés dans d'autres domaines[34]. La technologie est passée par paliers du statut de simple outil pratique à celui d'outil indispensable à l'exercice de nombreux domaines d'activités. Pour autant, le régime juridique de ces algorithmes n'a pas encore été fixé et laisse place à une forme d'insécurité juridique. L'insertion exponentielle des innovations technologiques au sein des outils visant à garantir l'ordre public interroge ainsi l'état du rapport entre la sauvegarde de l'ordre public, souvent désignée par le terme « sécurité », d'une part, et la protection des droits et des libertés, notamment du droit à la sûreté, d'autre part (**Section 1**).

14. Dans la perspective d'aborder cette étude, il convient par ailleurs de préciser certains concepts et définitions retenus des termes techniques du sujet (**Section 2**). Au regard des controverses entourant les derniers textes législatifs et réglementaires publiés en matière de sécurité publique[35], le lien étroit unissant la sécurité aux droits et libertés ne peut plus soulever de doute. Toutefois, la question porte, ici, davantage sur la signification actuelle du terme de sûreté en tant que droit et sur son rôle au sein des droits et libertés lorsque de nouvelles technologies viennent s'imposer afin de répondre aux exigences de sécurité publique. Aussi, il est nécessaire d'apporter des précisions quant au sens et au contenu des termes constituant le rapport entre la sûreté et la sécurité afin d'en comprendre l'évolution (**Section 3**). Ces éclaircissements effectués, il sera possible de présenter une première approche des enjeux juridiques liés à l'intronisation des drones aériens « augmentés » de sécurité publique au sein du rapport sûreté-sécurité. C'est ce

[34] De manière non-exhaustive : DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.* ; ALLARD (T.), Dossier sur « IA - L'intelligence artificielle pourra-t-elle un jour remplacer les politiques ? », *Sciences & Vie* n° 1255, avril 2022, pp. 64-81, spéc. pp. 66-67 ; VLASOV (A.) et BARBARINO (M.), « Sept contributions de l'IA au progrès de la science et de la technologie nucléaires », *Agence internationale de l'énergie atomique*, 2 décembre 2022 [en ligne] consulté en janvier 2023.

[35] De manière non exhaustive : DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, Paris, Le Seuil, 2010, 274 p. ; TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Paris, Dalloz, coll. « Les Sens du droit », 2017, 260 p. ; PARROT (K.) et ELMADJIAN (S.), Film « Sécurité globale, de quel droit ? », 29 janvier 2021 [disponible en ligne] ; PARROT (K.), « La proposition de loi sur la "sécurité globale" poursuit subrepticement une transformation sécuritaire de la politique pénale », *JCP G* n° 13, 29 mars 2021, 367 ; LAZERGES (C.), « Le droit à la sécurité a-t-il effacé le droit à la sûreté ? L'exemple de la loi « Sécurité globale » », *La Revue des droits de l'homme* n° 20, 2021, mis en ligne le 22 juin 2021 [en ligne], consulté le 7 juillet 2021 ; SAFI (F.), « La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement : Entre pérennisation et extension de l'exception… », *JCP G* n° 40, 4 octobre 2021, 1012 ; BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *op. cit.* ; LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *op. cit.*

renouvellement du lien entre sûreté et sécurité que cette étude tentera d'expliciter (**Section 4**).

Section 1 Objet de la recherche et intérêt du sujet

15. Au préalable, il convient de noter que le sujet de cette étude a été inspiré par les travaux menés dans le cadre d'un projet de recherche intitulé COOPOL mené en collaboration avec des industriels, des chercheurs et des organismes publics aux fins de développer des drones aériens couplés à des algorithmes d'analyse situationnelle pour un usage de sécurité publique[36]. Cette étude repose sur un objectif de démystification de l'emploi de drones aériens « augmentés » par les forces de l'ordre et les services de secours. Cette thèse entend offrir une vue d'ensemble des usages actuels et effectuer une analyse prospective des potentiels usages de cette technologie sans basculer dans une forme d'exagération ou un scénario de science-fiction. Cette étude tente d'analyser le sujet, plutôt technique, des technologies de surveillance que constituent les drones aériens « augmentés » de sécurité publique sous l'angle des droits et libertés. Il s'agit plus précisément d'étudier l'introduction de cette technologie au sein de l'espace public au regard du rapport entre sûreté et sécurité.

16. La question du rapport entre libertés et sécurité n'est somme toute pas des plus récentes mais n'en demeure pas moins tout à fait d'actualité comme en témoigne la loi relative à la responsabilité pénale et à la sécurité intérieure (RPSI)[37] (v. **n°198 et suiv.**). Ce texte vient s'ajouter à la longue lignée de ceux comportant des dispositions visant à préserver l'ordre public[38]. En outre, cette loi introduit un volet très attendu relatif à l'encadrement de l'utilisation des drones aériens de sécurité publique. Les drones aériens destinés aux forces de l'ordre et aux services de secours sont un sujet éminemment d'actualité soulevant des questions qui dépassent celles qui entourent habituellement les outils de surveillance (ex. caméras filmant l'espace public, IMSI catcher, etc.). Cette spécificité aérienne leur confère, en quelque sorte, un caractère « omniscient » où tout individu serait considéré comme susceptible de porter atteinte à l'ordre public. Ce caractère « omniscient » emporte dans son sillage une potentielle remise en question, entres autres, du principe de présomption d'innocence. Aussi, les drones aériens « augmentés » de sécurité publique

---

[36] Pour plus de détails, voir Annexe 2.

[37] Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, *JORF* n°0020 du 25 janvier 2022 [en ligne].

[38] Voir Annexe 3.

se distinguent d'autres outils de surveillance tant par leur mobilité que par leur discrétion.

17. Par ailleurs, l'association de drones aériens de sécurité publique à des algorithmes d'analyse d'évènements ne fait que renforcer l'effet de suspicion générale qu'induit l'analyse préventive d'événements. Ainsi, leur caractère novateur ne les empêche nullement de s'introduire dans le débat, pourtant ancien, du rapport entre sûreté et sécurité. Les drones aériens de sécurité publique engendrent un paradoxe en favorisant un « climat de sécurité » exigé par la société tout en remettant simultanément en cause l'application d'une liberté fondatrice de l'État de droit qu'est la sûreté. En d'autres termes, les drones aériens de sécurité publique associés à des algorithmes entendent contribuer à garantir l'ordre public en questionnant dans le même temps le maintien des garanties contre l'arbitraire étatique que la doctrine désigne aujourd'hui par la « liberté individuelle ». Ce paradoxe renferme, en outre, un conflit au sein des sources constitutionnelles entre les principes fondamentaux reconnus par les lois de la République auxquels appartient la liberté individuelle[39], d'une part, et les objectifs de valeur constitutionnelle qui intègrent la sauvegarde de l'ordre public[40], d'autre part.

18. L'évolution de la société entraine souvent l'introduction d'une nouvelle terminologie, qu'il s'agisse de l'apparition de termes ou expressions, ou de la modification d'un terme existant. Les mutations terminologiques sont une forme d'adaptation nécessaire à l'équilibre entre le mode d'expression et les modes de pensée actuelle. Elles sont le reflet linguistique de la société qui l'emploie. Ces changements de terminologie se retrouvent également dans les textes juridiques. Néanmoins, ils peuvent autant être bénéfiques qu'entrainer une forme de confusion ou de dégradation de l'interprétation du droit applicable. En ce sens, la professeure Mireille Delmas-Marty faisait référence à un brouillage terminologique d'origine politique entres les termes de sûreté et de sécurité[41].

19. Un constat récurrent au sein de la doctrine fait, en effet, état d'un glissement sémantique entre les termes de sûreté et de sécurité. Le caractère polysémique de ces termes peut en

---

[39] Depuis sa décision du 12 janvier 1977, le Conseil constitutionnel qualifie la liberté individuelle de principe fondamental reconnu par les lois de la République (C. const., Décision n° 76-75 DC, 12 janvier 1977, *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales*, Rec. p. 33 [en ligne]).

[40] La sauvegarde de l'ordre public reconnue comme ayant le statut d'objectif de valeur constitutionnelle par le Conseil constitutionnel lors de sa décision du 27 juillet 1982 (C. const., Décision n° 82-141 DC, 27 juillet 1982, *Loi sur la communication audiovisuelle*, Rec. p. 48 [en ligne]).

[41] DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 22.

l'occurrence expliquer ce flou dans leur emploi au sein des textes juridiques. Au-delà de la simple confusion d'ordre étymologique, ce constat révèle « un changement de paradigme : alors que la sûreté désigne une situation objective, une tranquillité, l'absence de trouble, la sécurité renvoie à un sentiment subjectif »[42]. Certains auteurs vont même jusqu'à dire que la « sûreté » a disparu au profit de la « sécurité ». Pourtant, le terme de « sûreté » renferme une importance capitale puisqu'il appartient au domaine des droits reconnus comme ayant valeur de principes constitutionnels fondamentaux à l'inverse de la « sécurité » qui, bien que souvent mentionnée dans les textes législatifs, ne revêt qu'un objectif de valeur constitutionnelle[43]. Or, le terme de « sûreté » présente un avantage non négligeable par son caractère dual : elle assure la garantie d'une protection de la personne contre l'arbitraire de l'État autant qu'une protection des personnes et des biens contre les actes criminels[44]. La « sûreté » affirme ainsi un principe associant la sécurité et les libertés. En outre, la « sécurité » est liée au maintien de l'ordre public qui comprend la protection des personnes et des biens. En d'autres termes, la « sécurité » a une visée strictement collective au contraire de la « sûreté » qui concerne les personnes de manière individuelle et collective[45].

20. La multiplication des termes désignant les droits et les libertés et, plus spécifiquement le droit à la sûreté, fait émerger un constat, somme toute assez naturel, qu'est celui d'une difficulté dans la compréhension de la terminologie employée. Le recours aux termes de « liberté individuelle » au singulier comme au pluriel vient attiser cette confusion de la maîtrise terminologique. La liberté individuelle désigne le droit à la sûreté quand les libertés individuelles renferment l'ensemble des libertés propres à chaque individu (ex. liberté d'aller et venir, droit à la vie, etc.) par opposition aux libertés collectives qui s'adressent à un groupe d'individus (ex. droit de manifestation, droit de grève, etc.). Il arrive également que les termes de « liberté individuelle » soient confondus avec ceux de « liberté personnelle ». Cette dernière peut être qualifiée de « liberté

---

[42] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », p. 84 *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, Bayonne, Institut universitaire Varenne, coll. « Colloques et essais », 2018, 302 p.

[43] Voir notamment : C. const., Décision n° 80-127 DC, 20 janvier 1981, *Loi renforçant la sécurité et protégeant la liberté des personnes*, Rec. p. 15 [en ligne] ; C. const., Décision n° 85-187 DC, 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie et dépendances*, Rec. p. 43 [en ligne] ; C. const., Décision n° 93-325 DC, 13 août 1993, *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*, Rec. p. 224 [en ligne].

[44] DELMAS-MARTY (M.), « État de droit, État de surveillance, surveillance sans État ? », p. 249 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*

[45] DEVOLVÉ (P.), « Sécurité et sûreté », *RFDA*, n°6,10 janvier 2012, p. 1085

matricielle »[46] en ce qu'elle comprend un ensemble de droits et libertés. La liberté personnelle se veut être une garantie de protection de la personne face aux ingérences publiques ou privées sur sa vie personnelle. Suite à la redéfinition du champ de la liberté individuelle par le Conseil constitutionnel, plusieurs des droits et libertés qui autrefois s'y inséraient se trouvent désormais protégés au sein de la liberté personnelle ; il s'agit du droit au respect de la vie privée, du droit de disposer de son corps, de la liberté d'aller et venir, de la liberté du mariage et du divorce, du droit au respect de la vie familiale ainsi que de l'inviolabilité du domicile.

21. En outre, il est troublant de constater le choix des termes de liberté individuelle pour désigner le droit à la sûreté dont les termes subsistent pourtant au sein de l'article 2 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789[47] (DDHC) et par conséquent demeurent au sein du Préambule de la Constitution Française. Faut-il alors comprendre que le droit à la sûreté, inscrit par les rédacteurs de la DDHC, comprenait un objectif plus large englobant la notion tant de sûreté institutionnelle que celle de sûreté individuelle ? Si tel est le cas, comment expliquer que la jurisprudence et la doctrine s'accordent sur les termes de liberté individuelle (s'insérant au sein des libertés individuelles) pour désigner le droit à la sûreté qui serait en fait tant une liberté individuelle qu'une limite à l'exercice des libertés individuelles dans un souci de conciliation permettant de garantir l'ordre public ? *A contrario*, faut-il y percevoir une volonté de moderniser la sémantique de cette notion juridique ? Le droit à la sûreté étant communément reconnu par la doctrine comme étant la garantie de l'exercice des autres droits et libertés il serait apparu comme logique de lui accorder comme nouvelle désignation celle de la liberté individuelle, première des libertés individuelles. Au vu des différentes mentions faites de la liberté individuelle ces dernières années (ex. le port du masque ou encore l'obligation du passe sanitaire lors de la pandémie), le constat peut être fait d'une utilisation « à tout va » de cette liberté sans connaitre les éléments qui la composent.

22. Ce constat est plus que jamais d'actualité et les confusions entourant les différentes notions se sont renforcées au fur et à mesure que l'emploi du terme de « sécurité » s'est inséré dans les textes juridiques visant principalement à englober toutes les actions effectuées par les forces de l'ordre et les services de secours. Les notions plus techniques relatives aux drones aériens et aux algorithmes ne prêtent pas à la même confusion mais peuvent souvent être mal maitrisées par le

[46] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, Paris, PUF, 2ème édition, 2020, 587 p., p. 328.

[47] Déclaration des droits de l'homme et du citoyen (DDHC) du 26 août 1789 [en ligne].

grand public. Il s'avère parfois même encore complexe de donner une définition juridique aux algorithmes tant le domaine est vaste. Néanmoins, il est possible d'en apporter une définition générale.

Section 2 Drones aériens « augmentés » : démystification terminologique

23. L'appréhension du sujet et la justification des termes employés dans le cadre de cette étude nécessite quelques apports d'ordre sémantique. En premier lieu, quelques précisions concernant l'emploi des termes « drones aériens » et « caméras aéroportées » s'imposent (§1). En deuxième lieu, il convient de démêler la notion d'algorithmes et de clarifier les autres terminologies qui y sont associées. En outre, il s'agira de justifier l'emploi des termes d'algorithmes « augmentés » dans le cadre de cette étude (§2).

§1. Les drones aériens ou aéronefs sans pilote à bord, des objets aux terminologies multiples

24. Les drones aériens font depuis quelques années l'objet d'une application étendue dans le domaine civil après avoir été pendant longtemps consignés au seul domaine militaire. Le sens commun les désigne généralement sous le terme « drone » ; pourtant la multiplicité de leurs applications fait qu'en réalité ce terme renferme de nombreuses définitions dont chacune s'est vue attribuer un terme plus technique. En outre, le terme « drone » ne désigne pas que les engins volants puisque que ceux-ci peuvent être conçus pour différents types d'environnement incluant les drones terrestres ainsi que maritimes[48].

25. Les drones aériens fascinent et font l'objet de nombreux articles tant dans les médias que dans les revues scientifiques. Le terme « drone » fait son apparition en 1935 et sa dénomination a pour origine le nom qui avait été donné à l'avion-cible automatisé du constructeur De Havilland, *Queen Bee* (Reine des abeilles), en raison de son bruit particulier, qui évoquait celui du faux bourdon ou *drone* en anglais[49]. Bien qu'étant le terme le plus communément employé, y compris dans certains articles scientifiques, le mot « drone » ne constitue qu'un terme générique dont

[48] Néanmoins, les drones terrestres et maritimes sont utiles pour d'autres types de missions que celles tenant aux missions de sécurité publique. Aussi, seuls les drones aériens ont vocation à être employés par les forces de l'ordre et les services de secours en France. Pour cette raison, l'étude se concentre exclusivement sur le recours à des drones aériens.

[49] MONNIER (E.), « Un premier drone militaire décolle en France », *Science et Vie* n°1198, juillet 2017, p. 130.

l'appellation est susceptible d'évoluer selon son contexte[50]. Plusieurs appellations existent pour désigner les drones[51], celles-ci n'étant pas toutes synonymes, par ailleurs.

26. Le terme « drone » ne dispose pas d'une définition légale. Néanmoins, il est possible de le définir comme un « véhicule ou engin mobile dont la caractéristique principale est l'absence d'une présence humaine à bord, qui n'est pas nécessairement un engin parfaitement autonome »[52]. Les institutions européennes proposent une définition des drones aériens qu'elles désignent par des « aéronefs sans pilote à bord pouvant être contrôlés soit de manière autonome soit par l'intermédiaire des commandes d'un pilote au sol ou dans un autre véhicule »[53]. Le législateur français désigne également le drone aérien sous les termes d'aéronef « sans personne à bord »[54] ou « sans équipage à bord »[55] ou « aéronef télépiloté »[56] (le terme « d'aéronef » étant plus communément employé dans d'autres textes juridiques) qu'il définit, plus sobrement, comme « un appareil capable de s'élever ou de circuler dans les airs »[57].

27. Toutefois, la documentation scientifique comme juridique préfère généralement des termes plus spécifiques qui varieront en fonction du contexte d'utilisation du drone aérien ou encore des finalités de son recours[58]. Ainsi, dans le cadre des drones aériens le droit européen désignera par UAV (*Unmanned Aerial Vehicle*) ou UAS (*Unmanned Air System*) tout drone capable de voler de manière autonome (drones préprogrammés ou automatisés), autrement dit sans le contrôle d'un télépilote. À l'inverse, le terme de RPAS (*Remotely Piloted Aircraft System*) sera préféré pour les drones demeurant sous le contrôle du télépilote, celui-ci pouvant être défini comme tout aéronef

---

50 GALLAIS (S.), *Cadre juridique de l'emploi des drones au combat*, *op. cit.*, p. 29.

51 CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.* ; CASSART (A.), *Droit des drones : Belgique, France, Luxembourg*, Bruxelles, éditions Bruylant, 2017, 187 p. ; LOBRY (A.), MÂZOUZ (A.) et WEIL (E.) (dir.), *Drones et droit*, Université de Cergy-Pontoise, coll. LEJEP, 2018, 183 p.

52 GALLAIS (S.), *Cadre juridique de l'emploi des drones au combat*, *op. cit*., p. 29.

53 European Union Aviation Safety Agency (EASA), Advance Notice of Proposed Amendment (A-NPA) 2015-10 - Introduction of a regulatory framework for the operation of drones, 31 July 2015, 41 p., p. 4. [en ligne].

54 Code de la sécurité intérieure (CSI), art. L611-3 ; Code de l'aviation civile (CAC), art. D136-1, D136-3, D136-7 ; Code des transports, art. L6214-1 et L6214-2 ; Code des postes et des communications électroniques (CPCE), L34-9-2.

55 Code des transports, art. L6111-1, L6232-12, L6232-13, L6214-2.

56 Code des transports, art. L6143-29.

57 Code des transports, art. L6100-1 al. 1er.

58 GALLAIS (S.), *Cadre juridique de l'emploi des drones au combat*, *op. cit.*, p. 29.

piloté à distance[59] disposant par conséquent d'une station de pilotage ainsi que d'un système de commande et de contrôle. Les instances internationales et européennes ont choisi le terme de RPAS pour désigner les drones aériens télépilotés afin de les différencier des UAV (ou UAS) où le terme « sans pilote » peut faire référence à une absence complète de pilote et n'inclurait par conséquent que les drones autonomes, autrement dit des objets aptes à évoluer sans intervention humaine[60]. La terminologie employée revêt par conséquent un caractère essentiel puisqu'elle permet de déterminer le régime juridique applicable[61].

28. Dans le cadre des drones aériens utilisés par les forces de l'ordre et les services de secours, il convient de mentionner que ceux-ci appartiennent à la catégorie des drones militaires qui devraient rester dans le cadre des RPAS[62] (ceux-ci ne pouvant faire l'objet d'une autonomie complète[63]). Par conséquent, les drones aériens à l'usage des forces de l'ordre et des services de secours ne prendront en compte que les aéronefs télépilotés, en d'autres termes ceux qui, sans disposer de pilote à bord demeurent sous le contrôle d'un télépilote[64].

29. La différenciation terminologique opérée entre les drones aériens témoigne d'une première volonté des institutions règlementaires de leur appliquer un cadre juridique adapté. Néanmoins, celle-ci ne suffit pas à répondre aux enjeux que peuvent engendrer les drones aériens suivant le type d'activités dont ils sont les sujets. Dans le cas des drones aériens à l'usage des forces de l'ordre et des services de secours, de nombreuses questions restent en suspens notamment quant aux conséquences qu'ils peuvent avoir sur l'exercice des droits et libertés. En outre, ceux-ci viennent entretenir le débat concernant le rapport entre sûreté et sécurité en devenant des éléments participant au *continuum* de sécurité que souhaitent renforcer les pouvoirs publics.

---

[59] CASSART (A.), *Droit des drones : Belgique, France, Luxembourg*, *op. cit.*, p. 17.

[60] CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p.246.

[61] WEIL (E.), « Drone civil : définition simple, qualifications multiples », pp. 11-24 *in* LOBRY (A.), MÂZOUZ (A.) et WEIL (E.) (dir.), *Drones et droit*, *op. cit.*

[62] CASSART (A.), *Droit des drones : Belgique, France, Luxembourg*, *op. cit.*, p. 166.

[63] Arrêté du 3 décembre 2020 relatif à la définition des scénarios standard nationaux et fixant les conditions applicables aux missions d'aéronefs civils sans équipage à bord exclues du champ d'application du règlement (UE) 2018/1139, *JORF* n°0298 du 10 décembre 2020, Annexe 1.3.1. [en ligne] : « À l'exception des aérostats captifs, l'exploitation autonome d'un aéronef est interdite ». Voir aussi : Direction Générale de l'Aviation Civile (DGAC), Guide « Usages des aéronefs sans équipage à bord : Catégorie spécifique », Édition 1, Version 1.7, 2 mars 2023 [en ligne].

[64] VACHER (P.), *Réglementation du pilotage de drones*, Toulouse, Éditions Cépaduès, 2016, 45 p., p. 9.

30. Le recours aux drones aériens par les forces de sécurité publique se double d'un autre enjeu de taille puisque ceux-ci sont destinés à intégrer ou à être coordonnés à des outils algorithmiques destinés à analyser une importante quantité de données afin d'aider les agents dans leur prise de décision. L'enjeu de ces algorithmes repose tant sur l'incidence liée à leur origine alors qu'ils « participent » à des activités régaliennes que sur les conséquences pour les personnes concernées des résultats qu'ils fournissent dans le processus décisionnel des agents de sécurité publique.

§2. Les technologies « augmentées » : les algorithmes et leurs typologies

31. Les drones aériens, à l'instar d'autres technologies, constituent potentiellement une source intarissable de données. Ils viennent s'ajouter à d'autres technologies dont l'objet repose également sur le traitement de données tels que les algorithmes. Ces derniers sont venus répondre aux besoins provenant de différents secteurs d'activités qui nécessitent le traitement et l'analyse d'un nombre important de données. Cette importante quantité de données se trouve généralement référencée sous les termes anglo-saxons de *Big Data* ou « masse de données ».

32. Il est désormais acquis que plus la technologie est développée et « sophistiquée » plus elle nécessite de données pour atteindre les objectifs fixés. Le néologisme d'« infobésité »[65], aussi dénommée « surcharge informationnelle »[66], décrit bien ce phénomène. L'infobésité repose sur « une consommation excessive d'informations »[67] ou aux besoins toujours croissants de collecter des données. Elle concerne principalement les médias sociaux dont la majeure partie de la population mondiale s'abreuve quotidiennement. Le terme d'infobésité peut toutefois commencer à s'appliquer à davantage de technologies au nombre desquelles se trouvent les caméras dites « intelligentes ».

---

[65] Le terme d'infobésité est défini par le Dictionnaire Larousse comme la « surabondance d'informations imputée aux chaînes d'information en continu, aux nouvelles technologies de la communication (Internet, téléphones portables, messageries, réseaux sociaux) et à la dépendance qu'elles créent chez l'utilisateur » [en ligne]. Voir sur ce sujet : SAUVAJOL-RIALLAND (C.), *Infobésité : Comprendre et maîtriser la déferlante d'informations*, Paris, Vuibert, 2013, 208 p. ; SAUVAJOL-RIALLAND (C.), « Infobésité, gros risques et vrais remèdes », *L'expansion Management Review* n° 152, 2014, pp. 110-118. [en ligne].

[66] HOANG (LN.) et EL MHAMDI (EM.), *Le fabuleux chantier : Rendre l'intelligence artificielle robustement bénéfique*, Paris, EDP sciences, 2019, 296 p., p. 56.

[67] *Ibid*.

33. De fait, les données sont une source inestimable d'informations recherchées dans tous les secteurs d'activités. En outre, elles peuvent notamment contribuer à l'intérêt général dans le cadre d'activités de sécurité publique. Toutefois, cette masse de données engendre d'importantes difficultés s'agissant de sa gestion. Aussi, ces données n'ont que peu de valeur lorsqu'elles sont prises isolément et nécessitent d'être agrégées en vue de devenir une source d'informations. Les algorithmes permettent de pallier, du moins partiellement, les difficultés de gestion d'une masse importante de données. En sélectionnant les données les plus pertinentes et en effectuant une analyse de celles-ci pour produire un résultat, ils participent au processus décisionnel de l'activité à laquelle ils ont été assignés[68].

34. Nonobstant l'utilisation quotidienne et grandissante des algorithmes, une grande partie du public s'avère rarement apte à en maîtriser la signification. De plus, la notion d'algorithme est souvent confondue avec celle d'intelligence artificielle (IA)[69], quand elle n'est pas confondue avec bien d'autres notions. Pourtant, l'IA et les algorithmes sont deux termes bien distincts mais néanmoins liés. En outre, il n'existe pas un type d'algorithme mais des types d'algorithmes. Dès lors, il convient d'expliciter ce qu'il faut entendre par algorithme afin d'identifier les enjeux engendrés selon le type utilisé et, dans le cadre de cette étude, ceux spécifiquement liés à un usage de sécurité publique.

35. La notion d'algorithme est ancienne puisqu'elle remonte à l'antiquité avec le premier algorithme élaboré par Eratosthène au III^e^ siècle avant J-C permettant de déterminer les nombres premiers. Le terme d' « algorithme » s'inspire du nom du mathématicien perse du IX^e^ siècle, Al-Khwârizmî[70]. Un algorithme peut être défini comme « une description d'étapes ou de règles à suivre pour obtenir un résultat à partir des données fournies en entrée »[71] ou encore comme « une séquence finie et non ambiguë d'opérations destinée à la résolution d'un problème »[72]. Il existe de nombreux

---

[68] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 13 : « Les progrès réalisés en informatique, notamment dans le domaine de l'intelligence artificielle, permettent désormais d'analyser de manière très efficace de grandes masses de données [et] extraire de ces big data des informations utiles à la prise de décision ».

[69] CNIL, « Comment permettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle », décembre 2017, p. 15 [en ligne] ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 15.

[70] PETIT (A.), « Préface », p. 1 *in* DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.*

[71] CNIL, « Définition - Algorithmes », [en ligne] ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 15.

[72] ISOARD (G.), « Algorithmes et biais cognitifs », p. 89 *in* DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.*

types d'algorithmes. Un algorithme « computationnel » (ou « numérique » ou « informatique »[73])[74] est un type d'algorithme utilisé et exécuté sur ordinateur[75]. La Commission nationale Informatique et Libertés (CNIL) offre plusieurs exemples de ce que peuvent accomplir les algorithmes[76]. Elle précise également que « pour qu'un algorithme puisse être mis en œuvre par un ordinateur, il faut qu'il soit exprimé dans un langage informatique, sous la forme d'un logiciel »[77]. Aussi, pour parvenir à répondre à la demande formulée, les algorithmes procèdent à partir d'un grand nombre de données.

36. Les données traitées par les algorithmes peuvent être à caractère personnel ou à caractère non personnel. Les DACP sont définies par le RGPD comme étant : « toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant […] ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[78]. Les données à caractère non personnel sont, quant à elles, définies par le règlement européen du 14 novembre 2018 relatif aux données à caractère non personnel et comprennent « toutes les données autres que les données à caractère personnel au sens de l'article 4, point 1), du RGPD »[79]. Les algorithmes engendrent, par conséquent, de nombreux enjeux juridiques concernant les données qu'ils traitent afin de fournir un résultat.

---

[73] Un algorithme informatique peut être défini comme « une suite d'instructions (traduisible sous forme de langage de programmation) que l'on opère sur les données initiales, en vue d'un résultat (résoudre un problème, répondre à un objectif). Un algorithme est à l'origine une manière de systématiser des actions par un ensemble fini d'opérations […] » (DELACROIX (F.), « Comprendre les algorithmes numériques », *InterCDI 273*, mai - juin 2018 [en ligne]).

[74] Par mesure de simplicité le terme d' « algorithme » sera utilisé seul pour faire référence aux algorithmes « computationnels » dans le cadre de cette étude.

[75] JEAN (A.), *Les algorithmes font-ils la loi ?*, Paris, Éditions de l'Observatoire/Humensis, 2021, 215 p., p. 214.

[76] De manière non-exhaustive : CNIL-LINC, Dossier « Intelligence artificielle » [en ligne] ; CNIL, « Intelligence artificielle, de quoi parle-t-on ? », *cnil.fr*, 25 mars 2022 [en ligne] ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, spéc. pp. 6-7.

[77] CNIL, « Définition - Algorithmes », *op. cit.*

[78] RGPD, art. 4.

[79] Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* 28 novembre 2018, [en ligne], art. 3.

37. Les algorithmes sont souvent confondus avec l'IA[80]. Ils sont certes étroitement liés mais ne sont pas pour autant des synonymes. Dernièrement, les sujets entourant l'IA sont indénombrables et ont envahi la sphère tant des médias généralistes que celle des publications scientifiques. Cet engouement pour le sujet de l'IA s'explique notamment par ses potentialités d'amélioration dans des domaines d'activités aussi nombreux que variés. La recherche scientifique dans le domaine du développement de cette technologie remonte au milieu du XXème siècle et a fait l'objet de nombreux rebondissements (avancées et abandons multiples)[81]. L'expression « intelligence artificielle » fait son apparition en 1957. Les algorithmes existent depuis tout aussi longtemps mais ont été mis en œuvre bien plus tôt. Ils sont une partie intégrante de l'IA. Ainsi, toute intelligence artificielle est composée d'algorithmes ; en revanche, tous les algorithmes ne sont pas des IA. Il semble nécessaire d'insister sur cette distinction tant par un souci de rigueur scientifique que par un besoin de compréhension et d'analyse du sujet.

38. Dans son avis du 7 avril 2022 concernant « l'impact de l'intelligence artificielle sur les droits fondamentaux », la Commission nationale consultative des droits de l'Homme (CNCDH) souligne l'importance dans le choix des termes employés en matière d'IA[82]. Elle constate une grande confusion suscitée par le recours de manière excessive à une terminologie qui ne reflète pas toujours la réalité des utilisations faites de cette technologie. Elle incite les acteurs du secteur public comme du secteur privé à limiter le recours à l'emploi du terme « intelligence artificielle » afin de contrer son incidence psychologique (méfiance) ou, à l'inverse, de confiance et d'acceptation excessives. Elle émet en ce sens une première recommandation invitant à « privilégier, dans la

---

[80] Il existe plusieurs définitions de l'Intelligence artificielle (IA). Dans ses travaux, la Commission d'enrichissement de la langue française définit l'IA comme un « champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines » (« Vocabulaire de l'intelligence artificielle », *JORF* n°0285 du 9 décembre 2018 [en ligne]). La CNIL définit cette technologie comme « un procédé logique et automatisé reposant généralement sur un algorithme et en mesure de réaliser des tâches bien définies » (CNIL, « Intelligence artificielle », [en ligne]) qu'elle complète par celle retenue par le Parlement européen qui considère comme constituant une IA « tout outil utilisé par une machine afin de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité » et regroupant celle-ci dans trois catégories incluant les approches d'apprentissage automatique, les approches fondées sur la logique et les connaissances, et les approches statistiques, l'estimation bayésienne, et les méthodes de recherche et d'optimisation (Parlement européen, « Intelligence artificielle : définition et utilisation », 29 mars 2021, [en ligne]).

[81] De manière non-exhaustive : TURING (A.), "Computing Machinery and Intelligence", *Mind* 59, October 1950 ; McCARTHY (J.), MINSKY (M.), ROCHESTER (N.) and SHANNON (C.E.), "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", Dartmouth University Summer Conference, August 31st 1955 [en ligne] ; LE CUN (Y.), *Quand la machine apprend*, Paris, Odile Jacob, 2019, 394 p. ; LE CUN (Y.), « Qu'est-ce que l'intelligence artificielle », *Le Point*, 16 mars 2017 [vidéo en ligne] ; IKONICOFF (R.), « Et la machine se mit à penser », *Sciences & Vie* Hors Série n° 290, mars 2020, pp. 8-15, spéc. pp. 12-13.

[82] CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, 7 avril 2022, *JORF* n°0091 du 17 avril 2022, 36 p., spéc. p. 4 [en ligne].

communication institutionnelle, une terminologie plus neutre et objective que l'expression "intelligence artificielle", telle que celle de "systèmes algorithmiques d'aide à la décision" (SAAD) »[83].

39. Le sujet de cette étude porte sur une forme de technologie de surveillance à l'usage de la sécurité publique (les drones aériens équipés de caméras) qui peut être associée à des algorithmes « augmentés ». Le terme « augmenté » a été choisi en référence à la désignation aujourd'hui employée par la CNIL concernant les caméras associées (ou équipées) d'algorithmes d'analyse d'images[84]. Ici, le terme « augmenté » doit être compris comme une technologie effectuant un lien entre les contenus « virtuels ou numérisés » et le monde réel. Cette technologie « augmentée », par l'intermédiaire d'algorithmes d'IA, permet d'analyser voire d'interpréter en temps réel des évènements apparaissant sous forme numérisée d'un espace physique (autrement dit réel) afin d'aider un agent dans sa prise de décision et ainsi accroître sa rapidité d'action. Dès lors, il faut aussi interpréter le terme « augmenté » dans son sens littéral comme étant un moyen technologique dont l'objectif repose sur l'augmentation de l'efficacité des tâches (en l'occurrence ici celles des missions de sécurité publique).

40. Ces quelques éclaircissements des termes techniques du sujet entendent faciliter leur ancrage dans le débat entourant le rapport entre sûreté et sécurité. Aussi, en vue d'acquérir une meilleure perception de la relation unissant la sûreté et la sécurité, il importe de déterminer ce que recouvre la notion de sûreté avant de tenter de définir les contours de la sécurité, clarifiant dans le même temps les notions tant d'ordre public que de sécurité publique.

Section 3 Le rapport entre la sûreté et la sécurité

41. Il est sans doute plus fréquent de faire référence au clivage entre libertés et sécurité. Cette étude se propose de partir du postulat que la sûreté, en constituant un rempart contre des décisions arbitraires étatiques, constitue la première des libertés. Le sujet porte alors délibérément sur le débat que suscite le rapport entre la sûreté et la sécurité. Le terme de « sûreté » fait souvent l'objet d'une confusion avec celui de « sécurité ». Il est vrai que les deux termes sont proches et qu'ils sont même

---

[83] *Ibid*.

[84] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

parfois employés comme synonymes[85]. Pour autant, les deux termes se distinguent sur le plan juridique à bien des égards[86]. De ce fait, l'étude du rapport entre sûreté et sécurité nécessite de définir au préalable les deux termes qui le composent. Il convient, dans un premier temps, de définir la notion de sûreté au sens des droits et libertés (§1). Dans un deuxième temps, il s'agira d'expliciter la notion d' « ordre public », à laquelle se rattache la « sécurité » pour ensuite tenter de trouver une qualification juridique au terme de « sécurité » de plus en plus usité dans les textes de loi non sans susciter de nombreuses confusions terminologiques (§2).

§1. Définition retenue de la sûreté

42. La « sûreté » regroupe plusieurs définitions qui méritent d'être précisées afin d'éviter toute confusion. Le terme de « sûreté »[87] revêt un caractère polysémique selon le complément de nom ou l'adjectif qui lui est attribué (A). Il existe différentes formes de sûreté : sûreté individuelle, sûreté institutionnelle, sûreté de l'État, sûreté publique, sûreté des personnes, sûreté personnelle, etc… La sûreté fait désormais place à de nouvelles terminologies au premier desquelles se trouve la « liberté individuelle » mais aussi parfois la « sécurité ». Les mutations terminologiques sont progressivement apparues dans les textes législatifs mais aussi dans la jurisprudence, principalement du Conseil constitutionnel. La jurisprudence constitutionnelle a du reste profondément évolué quant aux termes et au contenu des libertés individuelles usant désormais du terme de « liberté individuelle » pour désigner la « sûreté » (B).

---

[85] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, Paris, Dalloz, 4ème édition, 2020, 775 p., p. 331 ; DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 22 ; LÉCUYER (Y.) et LEMAIRE (F.), *Cours de droits humains et libertés*, Paris, édition Gualino, 2022, 690 p., p. 320 ; TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, pp. 67-80, spéc. p. 68 et pp. 81-101, spéc. p. 98 ; LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *JDJ* n°255, mai 2006, pp. 7-10 [en ligne] ; GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *RSC* n°2, 15 juin 2009, pp. 273-296 ; DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.* ; BEAUSSONIE (G.), « Droit à la sécurité contre droit à la sûreté. La liberté est-elle encore le principe ? », *Colloque sous la direction de GAVEN (J-C.) sur : Les ressorts de l'extraordinaire. Justice et police dans la fabrique de l'exception. Perspectives historiques et contemporaines*, Toulouse, 30 et 31 mars 2017, p. 2 [en ligne].

[86] OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, Paris, LGDJ, 7ème édition, 2019, 732 p., p. 313 : « La sûreté personnelle est la protection de la personne contre toute détention arbitraire […] Elle se distingue de la sécurité personnelle qui vise une protection à l'égard des agressions d'autres personnes » ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 331 : « La sûreté, […] suppose une limitation certaine du pouvoir politique et des forces de police afin de garantir la liberté individuelle, tandis que la sécurité contre les violences sociales appelle, au contraire, une extension de ces mêmes pouvoirs ».

[87] Est exclu du champ de cette étude la notion de sûreté désignant la garantie fournie par un débiteur à un créancier (sûreté conventionnelle, sûreté légale, gage ou encore hypothèque) pour l'exécution d'une obligation.

A. La sûreté, une notion polysémique

43. Bien qu'elle apparaisse dans plusieurs sources tant nationales qu'internationales, la sûreté ne fait que rarement l'objet d'une définition précise et se trouve souvent décrite par l'intermédiaire de « formules voisines, faisant appel à d'autres notions ou expressions, y compris celle de sécurité »[88]. La distinction entre sécurité et sûreté est, au premier abord, mal aisée et les deux termes sont fréquemment employés indifféremment tant dans le langage courant que juridique. Cette assimilation peut s'expliquer par leur origine commune venant du terme latin « *securitas* » qui signifie « sécurité » et fait référence à « l'état de celui qui n'a rien à craindre ou encore la situation qui ménage une protection »[89].

44. En droit public, notamment en matière de droits et libertés, la sûreté peut avoir différents objets selon qu'elle s'adresse à l'Homme ou qu'elle vise à protéger l'État et ce qui le compose. Dans le premier cas, l'Homme, en tant qu'individu, bénéficie d'un droit à la sûreté, aussi appelée sûreté individuelle, qui lui permet de se prémunir contre les agissements arbitraires de l'État (1). Dans le deuxième cas, il s'agit de protéger les institutions constitutives de l'État, d'où l'appellation de sûreté d'État ou de sûreté institutionnelle (2). Ce sont les moyens à mettre en œuvre en vue de protéger l'État contre toute menace susceptible de perturber son fonctionnement voire son existence.

1. La sûreté individuelle ou sûreté personnelle

45. La sûreté figure à l'article 2 de la DDHC, qui lui confère un caractère presque sacré la désignant comme l'un des quatre droits « naturels et imprescriptibles de l'Homme » avec « la liberté, la propriété et la résistance à l'oppression » et dont la préservation constitue « le but de toute association politique »[90]. Elle se prolonge aux articles 7, 8 et 9 de la Déclaration qui en garantissent le caractère primordial par l'introduction du principe de légalité des peines, du principe de non-rétroactivité de la loi pénale et du principe de la présomption d'innocence. Ainsi, l'article 7 de la Déclaration permet de mieux discerner l'objectif de la sûreté énonçant que « Nul homme ne peut

---

[88] DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.*

[89] GARRIDO (L.), « Le droit à la sûreté : un droit en danger ? » *in* GARRIDO (L.), (dir.), *Le droit à la sûreté : État des lieux, état du droit*, Paris, édition Cujas, 2012, 191 p., p. 5.

[90] DDHC, art. 2.

être accusé, arrêté ni détenu que dans les cas déterminés par la Loi, et selon les formes qu'elle a prescrites »[91]. Dès lors, la sûreté est le support de toutes les libertés individuelles[92] et est fondamentalement rattachée à la liberté individuelle[93]. Adoptée dans ce sens, cette « sûreté » s'adresse aux hommes pris individuellement raison pour laquelle elle peut être aussi désignée sous les termes de « sûreté individuelle »[94] ou de « sûreté personnelle »[95]. La sûreté individuelle désigne alors celle due à chaque citoyen[96].

46. L'article 8 de la Déclaration montagnarde de 1793 apporte un autre éclairage sur la notion de sûreté qu'elle définit comme « la protection accordée par la société à chacun de ses membres pour la conservation de sa personne, de ses droits et de ses propriétés »[97]. Il s'agit d'un droit créé par la société pour les individus et contre le pouvoir ; autrement dit, la sûreté se place comme rempart face aux décisions arbitraires de l'État. Elle est « le pivot de toutes les garanties de l'individu face à l'État sécuritaire »[98] et le « bouclier des autres libertés »[99]. Selon le professeur Jean Rivero, la sûreté condamne « au-delà même de la privation de liberté, toute forme arbitraire de

---

[91] DDHC, art. 7.

[92] LEBRETON (G.), *Libertés publiques et droits de l'homme*, Paris, Sirey, 8ème édition, 2008, 570 p., p. 380 : Le droit à la sûreté « revêt en effet une importance particulière dans une société démocratique. Car en proscrivant toute détention arbitraire, il permet aux individus de vivre libres, et d'exercer l'ensemble des autres libertés, tant publiques que politiques. En ce sens, le droit à la sûreté mérite ainsi d'être considéré comme le bouclier des autres libertés » ; CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, Paris, Dalloz, 2010, 751 p., p. 685 : « Ne pas être arrêté ni détenu arbitrairement, […] voilà le fer de lance de la liberté, et par conséquent, des régimes démocratiques qui la consacrent » ; FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, Paris, Dalloz, coll. Précis, 8ème édition, 2021, 978 p., spéc. pp. 204-205 ; Entretien de Robert Badinter déclarant que « le droit à la sûreté est la garantie des libertés individuelles du citoyen » (BADINTER (R.), « On tombe dans la répression administrée et on ouvre la voie à tous les soupçons », *Le Monde*, 27 janvier 2004 [en ligne] consulté le 19 juillet 2023).

[93] LEBRETON (G.), *Libertés publiques et droits de l'homme*, *op. cit.*, p. 380 : « On comprend dès lors pourquoi on l'appelle [le droit à la sûreté] traditionnellement, dans un raccourci saisissant, "la liberté individuelle" » ; FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 204 : « la liberté individuelle constitue le pendant du droit à la sûreté garanti par l'article 5 de la Conv.EDH » ; DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.* ; BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *Rec. Dalloz* n° 31, 21 septembre 2017, p. 1768 : « La sûreté, ce n'est alors rien d'autre, mais rien de moins, que la garantie que la liberté individuelle - au sens le plus large - demeure le principe dans la vie en société ».

[94] Plusieurs auteurs emploient les termes de « sûreté individuelle » : HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 332 ; DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.* ; BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *op. cit.*

[95] D'autres auteurs font référence à la « sûreté personnelle » : CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, spéc. pp. 685-702 ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 313 et suiv. ; FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 204.

[96] CORNU (G.) (dir.), *Vocabulaire juridique*, Paris, PUF, coll. Quadrige, 13ème édition, 2020, 1091 p., p. 995.

[97] Déclaration des droits de l'homme et du citoyen issue de la Constitution du 24 juin 1793, art. 8.

[98] BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *op. cit.*

[99] LEBRETON (G.), *Libertés publiques et droits de l'homme*, *op. cit.*, p. 380.

répression »[100].

2. La sûreté institutionnelle ou sûreté de l'État

47. La sûreté institutionnelle peut être définie comme la protection s'appliquant non pas à l'Homme mais à certaines institutions, installations ou systèmes d'intérêt pour la société. Elle peut être distinguée dans deux cas. En premier lieu, celui où elle protège l'État, ce qui lui vaut d'être parfois désignée sous les termes de sûreté de l'État, autrement dit, la sauvegarde de l'État. Elle peut aussi s'appliquer à des infrastructures reconnues comme indispensables à la survie de la nation telles que celles du domaine nucléaire ou encore des domaines électriques et gaziers. Certaines de ces infrastructures sont notamment désignées sous les termes d'opérateurs d'importance vitale (OIV). En deuxième lieu, celui où elle désigne les systèmes dont il faut assurer la sauvegarde (ex. la sûreté maritime, la sûreté aérienne ou encore la sûreté des approvisionnements)[101].

48. Un autre sens peut être donné à la sûreté institutionnelle, lorsque celle-ci est mise dans un contexte répressif où il s'agira davantage de protéger la société (ensemble de personnes) des menaces que peuvent présenter une personne contre elle. La sûreté institutionnelle, ou sûreté publique[102], à l'inverse de la sûreté individuelle, ne s'adresse pas à chaque individu mais aux individus dans leur ensemble. Il s'agit d'une sûreté collective qui par ses objectifs s'oppose à la sûreté individuelle. Cette terminologie est cependant plus rarement utilisée de nos jours, les textes lui préférant davantage le terme de sécurité.

B. Le champ du droit à la sûreté

49. Mis en lumière lors de la Révolution française de 1789, le droit à la sûreté constitue une garantie des droits[103]. En ce sens, il constitue « le fer de lance de la liberté, et par conséquent, des

---

[100] RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome II, Paris, PUF, 7ème édition, 2003, 269 p., n° 37.

[101] DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.*

[102] DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », issu du cours « Libertés et sûreté dans un monde dangereux », *Revue de synthèse* n° 3, tome 130, 6ème série, 2009, pp. 465-491 [en ligne] : « Si le droit à la sûreté est l'ébauche d'une vision libérale qui soumet l'État au droit, il porte en lui sa propre contradiction […] La référence expresse à la sûreté publique permet en effet de fonder les notions d'état d'urgence et d'état d'exception qui vont légitimer, en cas de danger pour la nation, des pratiques autoritaires, apparemment contraire à l'État de droit ».

[103] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 331 ; LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme », *RDP*, 1989, pp. 609 et suiv. ; GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.*

régimes démocratiques qui la consacrent »[104]. Bien qu'il constitue un « droit ancien de la première génération »[105], le droit à la sûreté ne sera pourtant reconnu que tardivement par le Conseil constitutionnel. Aujourd'hui, ce droit a acquis de nombreux fondements supra-législatifs depuis son inscription dans la DDHC. En premier lieu, le droit à la sûreté bénéficie d'un fondement constitutionnel, aux articles 2, 4, 7 et 9 de la Déclaration reprise dans le préambule de la Constitution du 4 octobre 1958[106]. Ce « bouclier » contre l'arbitraire a été consolidé par son inscription au sein même de la Constitution énonçant que « nul ne peut être arbitrairement détenu. L'autorité judiciaire gardienne de la liberté individuelle assure le respect de ce principe dans les conditions fixées par la loi »[107]. Aussi, le Conseil constitutionnel l'a élevé au rang de principe fondamental reconnu par les lois de la République lors de sa décision du 12 janvier 1977[108]. En deuxième lieu, le droit à la sûreté constitue un standard européen et dispose d'un fondement conventionnel international, à l'article 5 §1 de la Convention européenne des droits de l'homme[109] (Conv.EDH), à l'article 6 de la Charte des droits fondamentaux de l'Union européenne[110] (CDFUE), à l'article 3 de la Déclaration universelle des droits de l'Homme[111] (DUDH), ou encore à l'article 9 du Pacte international relatif aux droits civils et politiques[112] (PIDCP). Depuis sa décision du 18 juin 1971[113], la Cour européenne des droits de l'homme (CEDH), à l'instar du Conseil constitutionnel, reconnait l'importance de ce droit et insiste sur la nécessité de contrôler

---

104 CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 685.

105 *Idem*, p. 686.

106 Constitution de la Ve République du 4 octobre 1958, *JORF* 5 octobre 1958 [en ligne].

107 *Idem*, art. 66, al. 1er.

108 C. const., Décision n° 76-75 DC, 12 janvier 1977, *op. cit.*

109 Convention de sauvegarde des droits de l'homme et libertés fondamentales ou Convention européenne des droits de l'homme (Conv.EDH), Rome, 4 novembre 1950 [en ligne].

110 Charte des droits fondamentaux de l'Union européenne (CDFUE), 18 décembre 2000 révisée le 26 octobre 2012, 2012/C 326/02 [en ligne].

111 Organisation des Nations Unies (ONU), Déclaration Universelle des Droits de l'Homme (DUDH), Paris, 10 décembre 1948 [en ligne].

112 ONU, Pacte international relatif aux droits civils et politiques (PIDCP) du 16 décembre 1966 [en ligne] : Le texte mentionne toutefois les termes de « liberté » et de « sécurité » pour évoquer ce qui constitue en France la sûreté : « Tout individu a droit à la liberté et à la sécurité de sa personne. Nul ne peut faire l'objet d'une arrestation ou d'une détention arbitraire. Nul ne peut être privé de sa liberté, si ce n'est pour des motifs, et conformément à la procédure prévue par la loi » (art. 9, al. 1er).

113 CEDH, 18 juin 1971, *Affaire De Wilde, Ooms et Versyp c. Belgique*, n° 2832/66 et autre [en ligne].

scrupuleusement toute décision y portant atteinte[114].

50. Depuis la DDHC, les termes désignant le droit à la sûreté ont évolué pour faire désormais place à ceux de « liberté individuelle ». Aujourd'hui, cette terminologie semble prévaloir en droit bien que les deux notions cohabitent. À l'image de l'*Habeas corpus*[115] britannique[116], la liberté individuelle s'inscrit dans le prolongement du droit à la sûreté qui garantit à chaque individu de ne pas être arrêté ou détenu de manière arbitraire. Ainsi, la liberté individuelle constitue la première des libertés dans le sens où elle conditionne l'exercice des autres droits et libertés[117].

51. En dépit de son caractère essentiel et de sa valeur constitutionnelle, ce n'est que depuis la décision du 16 juin 1999[118] que le Conseil constitutionnel a fixé les contours de la liberté individuelle (désormais équivalente au droit à la sûreté). Le lien étroit entretenu entre le droit à la sûreté et la liberté individuelle, reconnus comme assimilables[119], a longtemps crée des émules au sein de la doctrine[120] quant à l'étendue du champ d'action de la sûreté et par conséquent aux garanties qu'elle confère aux autres droits et libertés[121]. En ce sens, le professeur Louis Favoreu mettait en garde contre les possibles confusions indiquant que la sûreté recouvrait le sens d'une

---

[114] La CEDH a confirmé sa volonté de protéger le droit à la sûreté dans l'arrêt *Engel et autres c. Pays-Bas* du 8 juin 1976, n° 5100/71 et autre [en ligne].

[115] *Habeas Corpus Act*, 1679 [en ligne] : « tout détenu doit pouvoir en appelé à un juge pour qu'il soit statué dans les meilleurs délais sur son cas ».

[116] BIOY (X.), *Droits fondamentaux et libertés publiques*, Paris, LGDJ, coll. Cours, 7ème édition, 2022, 1010 p., p. 695 ; DENIZEAU (C.), *Droit des libertés fondamentales*, Paris, Éditions Vuibert, 10ème édition, 2021, 448 p., p. 275 ; CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 686 ; DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 316 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 332 ; GARRIDO (L.), « Le droit à la sûreté : un droit en danger ? » *in* GARRIDO (L.) (dir.), *Le droit à la sûreté : État des lieux, état du droit*, *op. cit.*, p. 4 ; DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.*

[117] FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 199 : « Bouclier de toutes les autres libertés », la liberté individuelle constitue la clé de voûte es démocraties » ; DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 315.

[118] C. const., Décision n° 99-411 DC, 16 juin 1999, *Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs*, Rec. 75 [en ligne].

[119] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 316. Voir aussi : BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 695 : « Depuis la réduction de la notion juridique de liberté individuelle opérée par le Conseil constitutionnel, la sûreté est l'autre nom de « la » liberté individuelle » ; CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 687 : « le droit à la sûreté personnelle peut être compris comme synonyme de la liberté individuelle (au sens strict) de l'article 66 de la Constitution » ; DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.* : « La sûreté est […] intrinsèquement la liberté individuelle et inversement ».

[120] GARRIDO (L.), « Le droit à la sûreté : un droit en danger ? » *in* GARRIDO (L.) (dir.), *Le droit à la sûreté : État des lieux, état du droit*, *op. cit.*, p. 5.

[121] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 316 : « La liberté individuelle protégée par l'article 66 de la Constitution est désormais assimilable au droit à la sûreté […]. Elle correspond en substance […] au droit de ne pas être arrêté ou détenu de manière arbitraire ».

garantie générale contre l'arbitraire étatique, d'une part, ainsi que la garantie d'une « liberté-bouclier » assurant la protection « physique » des citoyens contre des décisions arbitraires de l'État[122]. Certains auteurs affirment que « dans une perspective classique, la sûreté recouvre essentiellement la liberté d'aller et venir et le droit de ne pas être arrêté ou détenu arbitrairement »[123]. Aujourd'hui, il s'agit de deux libertés individuelles distinctes (la liberté d'aller et venir et la liberté individuelle) « dotées chacune d'une source constitutionnelle propre, d'un contenu et d'un régime de protection spécifiques »[124]. Aussi, la doctrine s'accorde pour dire que le droit à la sûreté et la liberté individuelle sont équivalents et ont vocation à garantir à chaque individu le droit de ne pas être détenu arbitrairement[125]. Néanmoins, il convient de noter l'absence du terme « arrêté »[126] de l'article 66 de la Constitution (originairement mentionné par l'article 7 de la DDHC) qui pourtant dépasse la simple mesure restrictive de liberté, qui elle porte atteinte à la liberté d'aller et venir[127]. À l'inverse, la position de la CEDH ne laisse aucune place au doute[128] puisque « l'arrestation » demeure dans le champ d'application de l'article 5 §1 de la Conv.EDH[129].

52. Enfin, le droit à la sûreté se trouve au cœur des fondements du droit pénal en garantissant les grands principes de la loi et de la procédure pénale au rang desquels se trouvent la présomption d'innocence ou encore les règles applicables en matière de garde à vue et de détention provisoire. Il assure un équilibre essentiel du respect des droits de la personne dans son rapport avec l'ordre

---

122 FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, pp. 204-205.

123 HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 332.

124 FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 205.

125 De manière non-exhaustive : DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 276 : « Aujourd'hui, […] le droit à la sûreté s'entend donc *stricto sensu*, il désigne le droit de ne pas être arbitrairement détenu » ; DRAGO (G.), « Liberté individuelle et Constitution : Quels principes pour quels juges ? » *in Mélanges en l'honneur d'Yves Mayaud, Entre tradition et modernité : le droit pénal en contrepoint*, Paris, Dalloz, 2017, 846 p., pp. 529-540, spéc. p. 531 : « [La] réduction de la liberté individuelle à la seule source de l'article 66 de la Constitution la limite à la notion de sûreté personnelle et à la privation de liberté ».

126 PERERA (S.), *Le principe de liberté en droit public français*, Paris, LGDJ, Thèse, 2021, 606 p., p. 173 : « au moment de sa constitutionnalisation, la liberté individuelle a le sens de sûreté individuelle, c'est à dire de garantie contre les arrestations, détentions et pénalités arbitraires ».

127 Certains membres de la doctrine interprètent l'évolution de la jurisprudence du Conseil constitutionnel rattachant la liberté individuelle à l'article 66 de la Constitution comme ne protégeant les individus que contre les détentions arbitraires. Voir en ce sens : WACHSMANN (P.), *Libertés publiques*, Paris, Dalloz, 9ème édition, 2021, 1033 p. ; p. 658 : « Le droit de ne pas être victime d'une arrestation arbitraire et […] de ne pas être arbitrairement détenu dont il faut rappeler qu'ils sont désormais disjoints en droit français, le premier relevant de la liberté personnelle, le second de la liberté individuelle ».

128 Le professeur Patrick Wachsmann rappelle ainsi que : « pour la Cour européenne des droits de l'homme, l'arrestation reste incluse dans le champ de l'article 5 de la Convention, comme l'implique la lettre de l'article 5 §1 qui vise "l'arrestation" dans la moitié des causes de privation de liberté qu'il énumère ».

129 CEDH, 1er juillet 1961, *Lawless c. Irlande*, n° 332/57, n° 3 [en ligne] et CEDH, 7 mars 2013, *Ostendorf c. Allemagne*, n° 15598/08 [en ligne].

public. Pourtant, il semblerait qu'un glissement sémantique s'opère depuis plusieurs années entre la sûreté (issue de la DDHC) et la sécurité. Ainsi que le faisait remarquer le professeur Robert Badinter, lors des débats au Sénat en 2004, « à mesure que les décennies s'écoulaient […], singulièrement dans le discours politique, on affirmait constamment, avec de plus en plus de fermeté, que la sécurité était l'un des droits de l'homme inscrits dans la grande déclaration de 1789. […] Il s'est installé une sorte de confusion entre la sûreté […] et la sécurité des personnes et des biens »[130]. Force est de constater que le terme de sécurité, d'origine politique, vient progressivement se substituer à la notion de sûreté au sein même de la législation française entrainant de nombreuses confusions voire des contradictions. Il convient, par conséquent, de revenir sur le concept de sécurité pour tenter d'en donner une définition.

§2. La sécurité dans tous ses « états » : tentative de définition

53. Le terme « sécurité » est fréquemment employé dans la vie courante et désigne un vaste ensemble dont les significations divergent. La définition la plus communément accordée à la sécurité fait référence à la protection de l'intégrité physique des personnes et de leurs biens. En ce sens, le *dictionnaire Larousse* définit la sécurité comme « la situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration »[131]. Le *dictionnaire Robert*, quant à lui, désigne la sécurité comme « un état d'esprit confiant et tranquille d'une personne qui se croit à l'abri du danger » ou encore la « situation, état tranquille qui résulte de l'absence réelle de danger (d'orde matériel ou moral) »[132]. La sécurité peut aussi être définie comme « la situation de celui ou de ce qui est à l'abri des risques (s'agissant de risques concrets : agressions, accidents, atteintes matérielles…) »[133], il peut s'agir de la sécurité d'une personne (sécurité individuelle), d'un ensemble de personnes (sécurité publique) ou d'un bien. Pour autant, la sécurité ne doit pas se limiter à cette définition.

54. L'absence de base textuelle constitutionnelle - La sécurité est peu présente dans les textes « suprêmes » mais n'en est cependant pas absente[134]. En ce sens, le terme « sécurité » a été

[130] Propos de Robert Badinter issus du Sénat, Compte rendu intégral des débats du Sénat, 20 janvier 2004 [en ligne].

[131] Dictionnaire Larousse, [en ligne].

[132] Dictionnaire Le Robert, [en ligne].

[133] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 944.

[134] PIDCP, art. 9 (précité).

mentionné pour la première fois dans un texte juridique au sein de la Déclaration universelle des droits de l'homme de 1948[135]. Néanmoins, l'intention des rédacteurs de cette Déclaration reposait sur l'idée d'assurer des droits économiques et sociaux à tout individu et non d'une forme plus globale de sécurité de sa personne telle que la prévention des atteintes à son intégrité physique. En outre, il est intéressant de noter la mention d'un « droit à… », ici la sécurité, qui fait référence à un « droit-créance » ; en d'autres termes, « des pouvoirs reconnus aux individus d'exiger de […] la puissance publique, dans une perspective socialisante, un devoir d'intervention et d'assistance »[136]. La Constitution française, au sommet de la hiérarchie des normes, ne fait, pour sa part, aucune mention du terme de « sécurité » à l'inverse de la législation où l'on ne compte plus les textes visant à renforcer la sécurité du territoire contre les atteintes portées à l'ordre public. Certaines dispositions de la Déclaration pourraient être indirectement liées à la sécurité des personnes et des biens telles que celles affirmant la nécessité de la force publique[137] ou encore celles autorisant le législateur à « défendre les actions nuisibles à la société »[138]. Pour autant, la Déclaration universelle des droits de l'homme ne mentionne pas de manière explicite le terme de « sécurité ». Néanmoins, il est possible de rattacher le concept de sécurité à la notion d' « ordre public »[139].

55. La reconnaissance constitutionnelle - Ce n'est que par l'intermédiaire d'une catégorie juridique particulière, les objectifs de valeur constitutionnelle, que la sécurité a été reconnue par le Conseil constitutionnel. Par une décision du 27 juillet 1982[140], le Conseil constitutionnel intégrera pour la première fois de manière explicite les objectifs de valeur constitutionnelle au sein du bloc de constitutionnalité. À cette occasion, il a reconnu la sécurité comme étant une composante de l'ordre

---

[135] DUDH, art. 22 : « Toute personne, en tant que membre de la société a droit à la sécurité sociale […] » et DUDH, art. 25 : toute personne a « le droit à la sécurité en cas de chômage, de maladie, d'invalidité, de veuvage, de vieillesse ou dans les autres cas de perte de moyens de subsistance indépendants de sa volonté ».

[136] VIALA (A.), « Droits et libertés (Distinction) », p. 260 *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, Paris, PUF, coll. Quadrige, 2008, 1120 p.

[137] DDHC, art. 12.

[138] DDHC, art. 5.

[139] DDHC, art. 10 : « Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi ».

[140] C. const., décision n° 82-141 DC, 27 juillet 1982, *op. cit.* : « il appartient au législateur de concilier […] l'exercice de la liberté de communication telle qu'elle résulte de l'article 11 de la Déclaration des droits de l'homme, avec […] les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public, le respect de la liberté d'autrui et la préservation du caractère pluraliste des courants d'expression socioculturels ». Voir commentaires : AVRIL (P.) et GICQUEL (J.), *Pouvoirs* n° 23, novembre 1982, pp. 179-181 ; FAVOREU (L.), *Revue du droit public et de la science politique en France et à l'étranger* n° 2, avril 1983, p. 333 [§ 36, 42, 94, 96, 102, 104, 113, 127bis, 128] ; ETIEN (R.), *Revue administrative*, 1983.

public[141] consacrant ainsi l'objectif de valeur constitutionnelle relatif à la sauvegarde de l'ordre public[142]. Bien qu'ils ne soient nullement énoncés dans les textes constitutionnels, ils constituent la dernière catégorie du bloc de constitutionnalité à laquelle le Conseil constitutionnel a recours dans le cadre de son contrôle des lois[143]. Néanmoins, ils trouvent indirectement leur fondement au sein de la Constitution et reflètent généralement les objectifs déjà poursuivis par le législateur que le Conseil constitutionnel se « contente » de constitutionnaliser[144].

56. Les objectifs de valeur constitutionnelle appartiennent à une catégorie ouverte susceptible d'évoluer au fil des décisions du juge constitutionnel[145] et en accord avec la société. Pour autant, ils ne constituent pas des droits et libertés et tendent même à s'y opposer en autorisant le législateur à en limiter l'expression en vue de remplir ces objectifs[146]. En ce sens, l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public permet de restreindre l'exercice de la liberté d'aller et venir[147]. De par leur appartenance au bloc de constitutionnalité, ils ont incontestablement une valeur constitutionnelle. Dès lors, une loi qui s'opposerait à un objectif de valeur constitutionnelle serait reconnue comme inconstitutionnelle[148]. Toutefois, leur portée fait encore l'objet d'un débat[149] pour déterminer s'ils constituent seulement des objectifs à atteindre pour

---

141 LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, Éditions Studyrama, 9ème édition, 2021, p. 235.

142 Dans sa décision du 18 janvier 1995 (C. const., Décision n° 94-352 DC, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 [en ligne]), le juge constitutionnel reconnaitra un objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public comprenant notamment la prévention des atteintes à la sécurité des personnes et des biens pouvant être interprété « comme participant à la garantie du droit à la vie et du droit de propriété » (DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 156).

143 OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 179.

144 DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 30.

145 DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 30 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 197.

146 BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 150 ; DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 157.

147 C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*

148 C. const., Décision n° 93-333 DC, 21 janvier 1994, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*, Rec. p. 32 [en ligne].

149 HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 197 ; DE MONTALIVET (P.), *Les objectifs de valeur constitutionnelle*, Paris, Dalloz, coll. « Bibliothèque parlementaire et constitutionnelle », Thèse, 2006, 702 p.

le législateur[150] ou s'ils supposent « une obligation pour le législateur d'assurer la concrétisation de certains droits constitutionnels »[151].

57. Un rattachement à l'ordre public - Du fait de son caractère imprécis, le droit mentionne rarement le terme « sécurité » de manière isolée. Il est alors plus fréquent de le voir accompagné d'un complément de nom tels que « sécurité civile », « sécurité sociale », « sécurité publique », « sécurité intérieure », etc…[152] Certains de ces termes pouvant en comprendre plusieurs autres. En ce sens, la sécurité publique s'insère dans le cadre plus large de l'ordre public. Plus spécifiquement, la sécurité publique appartient à la dimension matérielle de l'ordre public, en d'autres termes à l'ordre sur la voie publique[153] (A).

58. Le champ de la « sécurité » - Aussi, une nouvelle terminologie a fait son apparition avec la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure[154] dite « LOPSI », celle de « sécurité intérieure ». Ces dernières années, le législateur a privilégié l'emploi de la « sécurité intérieure » à celui de « sécurité publique » sans pour autant l'y substituer. Dès lors, il convient d'apporter quelques éclaircissements sur ces termes afin de délimiter le champ de la « sécurité » dans laquelle s'insèrent les drones aériens « augmentés » destinés aux forces de l'ordre et aux services de secours (B).

---

[150] DENIZEAU (C.), *Droit des libertés fondamentales*, op. cit., p. 30 ; MAZEAUD (P.), « La place des considérations extra-juridiques dans l'exercice du contrôle de constitutionnalité » *in* 8ème séminaire des cours constitutionnelles tenu à Erevan du 2 au 5 octobre 2003, Les principaux critères de limitation des droits de l'Homme dans la pratique de la justice constitutionnelle, p. 4 [en ligne] : Les objectifs de valeur constitutionnelle peuvent être définis comme « des buts assignés par la Constitution au législateur pour rendre plus effectifs des droits et principes de valeur constitutionnelle ».

[151] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 156.

[152] DEVOLVÉ (P.), « Sécurité et sûreté », *op. cit.*

[153] BONNET (B.), « L'ordre public en France : de l'ordre matériel et extérieur à l'ordre public immatériel - Tentative de définition d'une notion insaisissable », p. 121 *in* DUBREUIL (C-A) (dir.), *L'ordre public*, Paris, CUJAS, coll. Actes et Études, 2013, 342 p.

[154] Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure (LOPSI), *JORF* du 30 août 2002 [en ligne].

A. La notion d'ordre public

59. La « loi suprême »[155], évoquée par Portalis, n'a pas toujours été désignée sous les termes d' « ordre public ». Avant la Révolution française, les « lois publiques » ou le « droit public » étaient les termes employés pour qualifier « l'instrument par lequel sont assurées, dans et par le droit, la défense et la promotion des valeurs et des intérêts qui structurent et conservent l'organisation sociale »[156]. L' « ordre public » fait son apparition lors de la chute de l'Ancien régime en intégrant successivement deux des textes les plus emblématiques du droit français que sont la DDHC[157] et le Code civil[158] de 1804. Désormais, l'ordre public est reconnu comme une notion fondamentale[159] et a pris une place prépondérante au sein de la hiérarchie des normes en droit français[160] devenant une norme intrinsèque au Droit[161].

60. Une notion complexe à définir - Proposer une définition juridique « générale » de la notion d'ordre public semble relever de la gageure tant la doctrine s'accorde pour constater les difficultés rencontrées pour en cerner les contours juridiques[162], celle-ci étant vouée à évoluer en

---

[155] LEBRETON (G.), « Ordre public », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, pp. 569-570 ; DEUMIER (P.) et REVET (T.), « L'ordre public », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, Paris, PUF, 6ème édition, 2019, 1696 p., p. 1119.

[156] DEUMIER (P.) et REVET (T.), « L'ordre public », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, pp. 1119-1122.

[157] DDHC, art. 10 (précédemment cité).

[158] C. civ., art. 6 : « On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs ».

[159] STIRN (B.), « Ordre public et libertés publiques » *in* SÈVE (R.), *L'ordre public*, Paris, Dalloz, coll. Archives de philosophie du droit, Tome 58, 2015, 474 p., p. 5 ; LEBRETON (G.), « Ordre public », pp. 569-570, *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.* ; BONNET (B.), « L'ordre public en France : de l'ordre matériel et extérieur à l'ordre public immatériel - Tentative de définition d'une notion insaisissable », p. 117 *in* DUBREUIL (C-A) (dir.), *L'ordre public*, *op. cit.*

[160] PICARD (E.), « Introduction générale : La fonction de l'ordre public dan l'ordre juridique », *in* REDOR (M-J.) (dir.), *L'ordre public : ordre public ou ordres publics ? Ordre public et droits fondamentaux*, Bruxelles, Bruylant, coll. Droit et justice, 2001, 436 p., p. 32.

[161] *Idem*, p. 36.

[162] MALAURIE (P.), *Les contrats contraires à l'ordre public : Étude de droit civil comparé : France, Angleterre, URSS*, Reims, Éditions Matot-Braine, Thèse, 1953, 278 p., p. 19 ; BERNARD (P.), *La notion d'ordre public en droit administratif,* Paris, LGDJ, coll. Bibliothèque de droit public, Thèse, 1962, 291 p., p. 2 ; BURDEAU (G.), *Traité de science politique*, Tome I, vol. 1, Paris, LGDJ, 3ème édition, 1980, 483 p., p. 291 ; PICARD (E.), *La notion de police administrative*, Tome II, Paris, LGDJ, coll. Bibliothèque de droit public, 1984, 926 p., pp. 540-544 ; PLANTEY (A.), « Définition et principes de l'ordre public », *in* POLIN (R.) (dir.), *L'ordre public*, Paris, PUF, 1996, 128 p., p. 27 ; LARRALDE (J-M.), « La constitutionnalisation de l'ordre public », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public oui ordres publics ? - Ordre public et droits fondamentaux*, Bruxelles, Bruylant, coll. Droit et justice, 2001, p. 213 ; LEBRETON (G.), « Ordre public », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, pp. 569-570 ; BONNET (B.), « L'ordre public en France : de l'ordre matériel et extérieur à l'ordre public immatériel - Tentative de définition d'une notion insaisissable », p. 117 *in* DUBREUIL (C-A) (dir.), *L'ordre public*, *op. cit.* ; STIRN (B.), « Ordre public et libertés publiques », *in* SÈVE (R.), *L'ordre public*, *op. cit.*, p. 5.

symbiose avec la société. En ce sens, le professeur Philippe Malaurie déclarait concernant la notion de l'ordre public que « nul n'a jamais pu en définir le sens, chacun en vante l'obscurité et tout le monde s'en sert »[163]. Aussi, le brouillard qui semble entourer la notion d'ordre public laisse planer une certaine inquiétude chez certains auteurs qui « pour les plus méfiants l'accusent même de véhiculer une idéologie sécuritaire hostile aux libertés »[164] ce que d'autres auteurs, tels le professeur Gilles Lebreton, jugent disproportionné[165]. En outre, il convient de noter que la détermination de son contenu dépend du contexte dans lequel l'ordre public est étudié ; en d'autres termes, de la branche du droit à laquelle il est fait référence[166].

61. Plusieurs auteurs se sont néanmoins évertués à proposer une définition de l'ordre public. Dans son sens général, l'ordre public est souvent défini comme « l'état social [d'un État] dans lequel la paix, la tranquillité et la sécurité publique ne sont pas troublées »[167]. Le professeur Patrick Wachsmann définit l'ordre public décrit comme « l'ensemble des valeurs dont les pouvoirs publics jugent indispensable d'imposer le respect à un moment déterminé »[168]. Dans le même sens, le professeur Gilles Lebreton définit l'ordre public comme « l'ensemble des règles que les autorités publiques (législateur, autorités administratives, juges voire organisations internationales) estiment indispensables pour sauvegarder la stabilité et les valeurs de la société. En ce sens, il est le principal instrument juridique du maintien de la paix sociale »[169]. L'ordre public, selon le conseiller d'État, Bernard Stirn, rassemble « les valeurs essentielles du consensus social et du système juridique »[170].

---

[163] MALAURIE (P.) cité par GAUTIER (M.), « L'ordre public », *in* AUBY (J-B), *L'influence du droit européen sur les catégories du droit public*, Paris, Dalloz, 2010, 1006 p., p. 317.

[164] LEBRETON (G.), « Ordre public », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, pp. 569-570.

[165] *Idem* : L'ordre public s'avère, en réalité, « plus clair qu'on ne le croit, il concilie sa diversité d'expressions avec une indéniable unité conceptuelle. Et moins dangereux qu'on ne le craint, il protège autant qu'il les limite les droits fondamentaux de la personne humaine ».

[166] En ce sens, le professeur Etienne Picard soulignait que « pour répondre à la question du contenu de l'ordre public non autrement spécifié, il faudrait donc rendre compte de l'ordre public sous toutes ces manifestations [cf. différentes branches du droit] à la fois ; il faudrait tenter d'en fournir une représentation unitaire qui laisserait cependant la place à ces spécificités disciplinaires » (PICARD (E.) « Introduction générale », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public oui ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, pp. 17-61, spéc. p. 20).

[167] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 714.

[168] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 69.

[169] LEBRETON (G.), « Ordre public », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, pp. 569-570. Le professeur Jean Rivero associait la notion d'ordre public « aux assises matérielles de la vie sociale » (RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome I, Paris, PUF, 9ème édition, 2003, 271 p., p. 229).

[170] STIRN (B.), « Ordre public et libertés publiques », p. 5, *in* SÈVE (R.), *L'ordre public*, *op. cit.*

Enfin, les professeures Stéphanie Hennette-Vauchez et Diane Roman énoncent que la notion d'ordre public peut être définie comme « permettant de concilier l'exercice des droits et libertés avec les exigences de la vie en société »[171]. La transgression constitue l'essence de l'ordre public et permet d'ouvrir la conciliation entre les libertés reconnues comme fondamentales et les besoins exprimés par la société. L'ordre public constitue une notion-cadre à laquelle le législateur a souvent recours dans sa mission d'organisation de la conciliation entre les différents droits garantis.

62. Cette multiplicité des définitions de l'ordre public serait vraisemblablement liée à la « relative mais indéniable indétermination du contenu de l'ordre public ; […] le caractère d'ordre public d'une norme est inhérent au fait qu'elle mette en œuvre un intérêt ressortissant aux valeurs sociales essentielles »[172]. Ainsi, l'ordre public n'est pas un état social figé dans le temps mais évolutif[173] où « il varie tant dans son contenu que dans sa place dans la hiérarchie des normes, au gré des transformations de la société et des attentes de celle-ci »[174]. Pour le professeur Baptiste Bonnet, l'ordre public n'a pas de définition fixe mais des « contours ». Il précise ainsi que son contenu ne peut être déterminé « qu'au moment où apparaît le comportement humain qui présente un risque social ou au moment où dans une société donnée, on considère […] que tel comportement présente désormais un risque social […] et que l'on décide, par conséquent de l'interdire ou tout du moins de l'encadrer »[175].

63. Une notion évolutive - Aussi, il convient de noter que la notion d'ordre public ne se limite plus aujourd'hui à sa seule dimension « matérielle et extérieure »[176] et comprend désormais

---

171 HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 225.

172 DEUMIER (P.) et REVET (T.), « L'ordre public », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, pp. 1119-1121. Les auteurs mentionnent en ce sens que « M. Philippe Malaire a recensé pas moins de 22 définitions, auxquelles il a ajouté une 23e, la sienne ».

173 MALAURIE (P.), « Rapport de synthèse » *in* REVET (T.) (dir.), *L'ordre public à la fin du XXème siècle*, Paris, Dalloz, 1996, 111 p., pp. 105-111, spéc. p. 107.

174 LEBRETON (G.), « Ordre public », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, pp. 569-570.

175 BONNET (B.), « L'ordre public en France : de l'ordre matériel et extérieur à l'ordre public immatériel - Tentative de définition d'une notion insaisissable », p. 118 *in* DUBREUIL (C-A) (dir.), *L'ordre public*, *op. cit.*

176 Tel que l'affirmait le Doyen Maurice Hauriou pour qui « l'ordre que les administrations publiques ont pour but de maintenir est l'ordre matériel. Les autorités administratives pourchassent le désordre dans ses manifestations extérieures, dans la rue, dans les lieux publics, mais elles ne peuvent prétendre réaliser l'ordre moral, l'ordre à l'intérieur des consciences. Elles sont pour cela radicalement incompétentes, car, ne disposant pour le maintien de l'ordre que de moyens matériels, si elles les mettaient en œuvre pour les consciences, elles verseraient dans l'inquisition et dans l'oppression » (HAURIOU (M.), *Précis de droit administratif et de droit public* [1933], Paris, Sirey, 12ème édition, 2003, 1150 p., p. 58).

une dimension « immatérielle » afin d'y intégrer des « valeurs » communes[177]. Désormais, la doctrine admet la double dimension de l'ordre public[178] issue des évolutions de la notion d'ordre public. L'ordre public, pris dans sa dimension matérielle, était défini par le Doyen Maurice Hauriou comme « un état de fait opposé au désordre, état de paix opposé à l'état de trouble »[179]. Il peut également être défini comme « l'établissement dans la collectivité des conditions qui assurent le plein épanouissement de l'individu »[180]. L'ordre public matériel a pour objet « d'assurer à l'État le monopole de la violence physique légitime »[181]. La notion d'ordre public est étroitement liée à celle de l'intérêt général mais s'en distingue[182] par son caractère plus étroit et plus strict. Dans le cadre de cette étude, seule la dimension matérielle de la notion d'ordre public sera abordée dans le souci de ne traiter que les aspects relatifs à la sécurité publique et de ne pas faire intervenir le champ moral nécessairement inadapté aux outils numériques. Les technologies « augmentées » à l'usage de la sécurité publique présentent des résultats dont les critères prédéfinis ne sont en effet pas supposés comporter de dimension morale. Dans l'hypothèse où cela serait techniquement possible, l'éventualité de voir une dimension morale dans le programme de ces technologies « augmentées » n'est pas non plus souhaitable dans la mesure où elle relèverait de la seule appréciation de ses concepteurs.

64. La notion « d'ordre public » apparaît rarement dans les textes juridiques français y compris dans la Constitution française qui n'y fait référence que dans son Préambule par l'intermédiaire de la DDHC[183]. La notion d'ordre public s'est essentiellement construite au travers de la jurisprudence du Conseil constitutionnel et du Conseil d'État[184]. Le Conseil constitutionnel n'a eu de cesse de rechercher si des dispositions législatives relatives à la sauvegarde de l'ordre

---

[177] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 226.

[178] *Idem*, p. 241 ; BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 236 ; BONNET (B.), « L'ordre public en France : de l'ordre matériel et extérieur à l'ordre public immatériel - Tentative de définition d'une notion insaisissable », p. 120 *in* DUBREUIL (C-A) (dir.), *L'ordre public*, *op. cit.*

[179] HAURIOU (M.), *Précis de droit administratif et de droit public* [1933], *op. cit.*, p. 549.

[180] BERNARD (P.), *La notion d'ordre public en droit administratif, op. cit.*, p. 49.

[181] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 69.

[182] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 235.

[183] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, Paris, LGDJ, Thèse, 2014, 517 p., p. 29. Voir aussi : BURG (M.), *Droit fondamental et opérationnel du maintien de l'ordre public*, Nancy, PUN, coll. « Pour ainsi dire », 2020, 177 p., p. 20.

[184] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 235

public étaient proportionnées à l'exercice des droits et libertés[185]. La notion d'ordre public s'est principalement imposée par la jurisprudence du Conseil constitutionnel, qui lui a reconnu le statut d'objectif de valeur constitutionnelle. Dans sa décision du 20 janvier 1981, il avait ainsi jugé que la liberté individuelle et la liberté d'aller et venir devaient « être conciliées avec ce qui est nécessaire pour la sauvegarde des fins d'intérêt général ayant valeur constitutionnelle comme le maintien de l'ordre public »[186]. Il a confirmé cette exigence constitutionnelle lors de sa décision du 25 janvier 1985 évoquant « la sauvegarde de l'ordre public sans lequel l'exercice des libertés publiques ne saurait être assuré »[187]. Aujourd'hui, l'ordre public bénéficie d'une définition légale, inspirée par la loi municipale du 5 avril 1884, au sein du Code général des collectivités territoriales (CGCT) qui le définit comme « le bon ordre, la sûreté, la sécurité et la salubrité publiques »[188]. L'ordre public repose sur deux piliers que sont la prévention des infractions et la répression pénale[189]. Il s'oppose à la liberté de principe lorsque cela est nécessaire.

65. Dès lors, il est surprenant que le terme de « sécurité » soit régulièrement substitué à celui d' « ordre public » dont la conciliation avec les libertés constitue pourtant le fondement de l'État de droit. Pour rappel, en droit public français, la « sécurité » est traditionnellement reconnue comme dépendante de l'ordre public. Aussi, cette « sécurité », inlassablement répétée dans les discours politiques, voudrait rassembler les notions de libertés, comme sécurité juridique, et d'ordre public, comme sécurité matérielle des individus qui s'opposent pourtant à l'exercice de ces mêmes libertés. En ce sens, le professeur Pascal Mbongo notait que dans « le lexique contemporain, c'est l'ordre public qui devient une dépendance, une "composante", de la sécurité »[190] entrainant à la fois une confusion d'ordre terminologique et d'objet de l'ordre public. Il semble alors nécessaire d'éclaircir ce concept de « sécurité ». Pour ce faire, il convient de définir les contours d'une notion propre à

---

[185] À titre d'exemple lors de sa décision du 12 janvier 1977 (C. const., Décision n° 76-75 DC, 12 janvier 1977, *op. cit.*), reconnaissant le titre de principe fondamental de valeur constitutionnelle à la liberté individuelle, le juge constitutionnel a estimé que les dispositions de la loi qui lui étaient soumises octroyaient des pouvoirs mal définis et disproportionnés aux officiers de police judiciaire.

[186] C. const., Décision n° 80-127 DC, 20 janvier 1981, *op. cit.*, cons. 58.

[187] C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.*, cons. 3 et 4.

[188] CGCT, art. L. 2212-2.

[189] LAMY (F.), « La production de la sécurité publique », pp. 17-34, spécifiquement p. 18 *in* SÈVE (R.), *L'ordre public*, *op. cit.*

[190] MBONGO (P.), « La "sécurité", brève histoire française d'un camaïeu », p. 19 *in* MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, Paris, édition L'Harmattan, 2012, 276 p.

l'ordre public celle de la sécurité publique, et d'éclaircir la notion de sécurité intérieure à laquelle le législateur fait désormais plus fréquemment référence.

B. Les notions de sécurité publique et de sécurité intérieure

66. L'emploi du terme « sécurité », pris isolement ne dispose pas d'une valeur juridique. Il convient donc de lui associer un adjectif afin de définir son objet. Cependant, le choix de l'adjectif approprié n'est pas des plus aisé, comme en témoignent nombres de textes, législatifs comme réglementaires, usant de termes très hétérogènes pour accompagner celui de « sécurité ». Ainsi, la sécurité peut être intérieure, publique, civile, nationale[191], quotidienne, extérieure… Parmi ce florilège de termes, deux d'entre-eux semblent convenir à l'étude des drones aériens dotés d'algorithmes « prédictifs » destinés aux forces de l'ordre et aux sapeurs-pompiers : ceux de « sécurité publique » et de « sécurité intérieure ».

67. Notion de sécurité publique - Selon le professeur Olivier Gohin, « par sécurité dans la Constitution de 1958, il faut entendre la sécurité publique »[192] par opposition à la sécurité privée. La sécurité publique est un des éléments constitutifs de l'ordre public et se caractérise « par l'absence de périls pour la vie, la liberté ou le droit de propriété des individus »[193]. Elle est celle assurée par les autorités publiques de l'État. Plus précisément, la sécurité publique renvoie à la sécurité sur la voie publique (en d'autres termes, les missions habituellement confiées aux agents des forces de l'ordre) ainsi qu'à la prévention de la délinquance[194]. Il s'agit d'une sécurité collective qui « s'inscrit dans une logique de service public à travers des prérogatives de puissance publique »[195]

---

191 Il convient d'apporter quelques précisions d'ordre sémantique quant au terme de sécurité nationale. La loi de programmation militaire du 29 juillet 2009 a introduit la notion de sécurité nationale (autrefois appelée défense nationale) qu'elle définit comme « une action politique cohérente et construite à long terme » (Code de la défense, art. L. 1111-1). Néanmoins, les deux termes ne sont pas synonymes, la défense nationale s'axant sur une stratégie de réaction tandis que la sécurité nationale porte davantage sur une volonté d'anticipation et sur le renseignement (PRADEL (J.), « Préface » in DE DAVID BEAUREGARD-BERTHIER (O.) et TALEB-KARLSSON (A.) (dir.), *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?*, Bruxelles, édition Bruylant, 2017, 279 p, p. 8). À l'inverse de la défense nationale qui consiste en des actions menées en situation concrète, la sécurité nationale repose sur une volonté de prévention des actes susceptibles de menacer le bien-être des individus et des institutions de l'État.

192 GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, Vol. 6, 2021, 318 p., pp. 19-29, spéc. p. 19.

193 CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 945.

194 LAMY (F.), « La production de la sécurité publique » *in* SÈVE (R.), *L'ordre public*, *op. cit.*, pp. 17-34, spéc. p. 19.

195 GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 19-29, spéc. p. 19.

intégrant les mesures de police administrative. Dès lors, elle constitue l'un des objectifs de la police administrative avec ceux de la tranquillité et de la salubrité publique.

68. Les missions de la sécurité publique sont définies dès le premier article du CSI[196]. Le rapport au Président de la République relatif à l'ordonnance du 12 mars 2012 précise le champ de la sécurité publique qui « consiste en la protection des personnes, des biens et des institutions contre des atteintes délibérées, pénalement répréhensibles, allant de simples infractions jusqu'aux actes de terrorisme »[197]. Aussi, le CSI précise que la sécurité civile « concourt à la protection générale des populations, en lien avec la sécurité publique »[198]. En ce sens, le conseiller d'État, Francis Lamy, rappelle que la sécurité civile s'insère, au sens général, dans la notion de sécurité publique et, au sens juridique, dans la notion de police administrative générale[199]. En conséquence, les missions exercées par les sapeurs-pompiers font partie intégrante de la sécurité publique.

69. Aujourd'hui, les termes de « sécurité publique » sont peu usités dans la législation actuelle comme au sein de la doctrine. Ceux de « sécurité intérieure » sont plus communément employés du fait qu'ils sont plus généraux et représentatifs des activités de sécurité exercées aujourd'hui sur le territoire[200]. Il arrive même que la « sécurité publique » et la « sécurité intérieure » fassent l'objet d'un emploi alternatif entrainant cependant des difficultés d'appréhension du sujet, comme le souligne le professeur Xavier Latour[201].

70. Notion de sécurité intérieure - Concept né dans les années 1980 suite à de multiples attentats, la notion de « sécurité intérieure » connait un regain d'utilisation au début des années

---

196 CSI, art. L. 111-1, al. 2 : « L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens ».

197 Rapport au Président de la République relatif à l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure, *JORF* n°0062 du 13 mars 2012 [en ligne].

198 CSI, art. L112-1.

199 LAMY (F.), « La production de la sécurité publique » *in* SÈVE (R.), *L'ordre public*, *op. cit.*, pp. 17-34, spéc. p. 19.

200 Aujourd'hui, les déclarations gouvernementales évoquent un effort collectif de mise en œuvre de la sécurité impliquant tous types d'acteurs. Voir en ce sens le Livre Blanc sur la sécurité (évoqué précédemment).

201 Dans son article étudiant l'introduction du Code de la sécurité intérieure, le professeur Xavier Latour soulève notamment la question de l'appartenance de la sécurité privée dans le champ de la sécurité publique où il définit comme étant « publique la sécurité directement assumée par l'État conformément à l'article 12 de la DDHC, grâce aux effectifs de police et de gendarmerie » (LATOUR (X.), « Des activités privées de sécurité et des agences de recherche privées dans le Code de la sécurité intérieure » *in* MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, *op. cit.*, p. 194).

2000[202]. Les termes de « sécurité intérieure » sont apparus assez récemment dans les textes juridiques, les premiers datant des années 1990[203]. L'expression de « sécurité intérieure » apparait pour la première fois dans la législation par la loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure[204] dite « LOPSI ». Bien que le législateur en fasse désormais régulièrement l'usage[205] il est encore difficile de définir la notion de « sécurité intérieure »[206]. Ainsi, cette dernière ne fait l'objet d'aucune définition juridique et ce malgré les efforts employés par la doctrine. Aussi, le CSI n'a pas dérogé à la règle en maintenant un flou juridique autour de la notion de sécurité intérieure[207] dérivée des textes législatifs et réglementaires l'ayant précédé qui n'apportaient pas d'éléments concrets à sa définition. Néanmoins, la notion de « sécurité intérieure » comprend des « éléments juridiques, au premier rang desquels figure la notion d'ordre public, essentielle à la sécurité publique, elle-même composante de la sécurité intérieure »[208].

71. Certains auteurs se risquent à donner une définition de la sécurité intérieure comme étant une « absence de trouble et d'inquiétude, paix, calme et tranquillité qui règnent, au sein d'un État, pour ses ressortissants et habitants »[209] ou plus simplement un objectif qui repose principalement sur la lutte contre la criminalité (prévention et répression). La définition de la sécurité intérieure peut indirectement être déduite au travers des définitions des différents types de sécurité qu'en

---

[202] Voir notamment : Décret n° 2002-890 du 15 mai 2002 relatif au Conseil de sécurité intérieure, *JORF* n°113 du 16 mai 2002 [en ligne], et plus particulièrement la loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure (LOPSI), *op. cit.* et loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), *JORF* n°0062 du 15 mars 2011 [en ligne].

[203] Décret n° 91-903 du 10 septembre 1991 portant organisation de l'Institut des hautes études de la sécurité intérieure, *JORF* n°214 du 13 septembre 1991 [en ligne] et décret n° 97-1052 du 18 novembre 1997 portant création du Conseil de sécurité intérieure, *JORF* n°268 du 19 novembre 1997 [en ligne].

[204] Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure (LOPSI), *op. cit.*

[205] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, Paris, LGDJ, Thèse, 2011, 493 p., p. 14.

[206] *Idem* ; DURAND (F.), « La notion de sécurité intérieure à travers les livres blancs et le code de la sécurité intérieure », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 239-252, spéc. p. 239.

[207] LATOUR (X.), « Le périmètre du Code de la sécurité intérieure, entre ordre et désordre » *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, p. 50 ; GOHIN (O.) et LATOUR (X.) (dir.), *Code de la sécurité intérieure*, Paris, LexisNexis, 2021, 2026 p., Préface : « Aussi étonnant que cela soit, la sécurité intérieure, dans le code de la sécurité intérieure, n'a pas de définition qui soit explicite et elle ne pouvait recevoir légalement de ce code une telle définition ».

[208] DURAND (F.), « La notion de sécurité intérieure à travers les livres blancs et le code de la sécurité intérieure », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 239-252, spéc. p. 241.

[209] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 945.

donne le CSI ainsi que des textes législatifs qui le composent[210]. Aussi, si aucun des quatre *Livres blancs* consacrés à la sécurité n'offre de définition explicite de la notion de « sécurité intérieure » ceux-ci proposent d'éléments permettant d'en expliciter le contenu.

72. Aujourd'hui, l'usage de cette notion dans les documents gouvernementaux et textes législatifs traduit principalement une volonté des pouvoirs politiques successifs d'introduire de manière pérenne des acteurs issus du secteur privé au sein des actions visant à garantir l'ordre public[211]. Aussi, la préférence accordée à l'emploi des termes de « sécurité intérieure » sur ceux de « sécurité publique » et de « sécurité civile » par le législateur témoigne également de la tendance à satisfaire les demandes de l'exécutif.

73. Choix terminologique du sujet - Le choix d'adopter la notion de « sécurité publique » s'explique tant par les acteurs ayant l'usage des algorithmes « prédictifs » des drones aériens (principalement les forces nationales de l'ordre et dans une moindre mesure les sapeurs-pompiers) que par la volonté d'affirmer le besoin de maintenir au sein de la puissance régalienne le devoir d'assurer l'ordre public. En ce sens, l'analyse des *Livres blancs* sur la sécurité, effectuée par Franck Durand, mène à définir la sécurité intérieure comme résultant « de l'action conjointe des forces nationales de police et de gendarmerie - seules qualifiées de forces de sécurité intérieure - des polices municipales et de la sécurité privée »[212]. Le choix des termes de « sécurité publique » permet ainsi de limiter aux seules forces de l'ordre autorisées à faire usage de drones aériens (v. **n° 210**). Aussi, les drones aériens sont également destinés à un usage par les sapeurs-pompiers[213] qui appartiennent à la sécurité civile et sont placés sous le contrôle du ministère de l'Intérieur où ils assurent des missions de secours, de protection contre les incendies et les périls ou accidents de toute nature portant atteinte à la sécurité publique[214]. Dès lors, l'action des sapeurs-pompiers prend part à la sécurité publique. Aussi, il convient de noter que la définition des acteurs de la sécurité intérieure diffère entre le CSI qui inclut la sécurité civile, d'une part, et les *Livres blancs* relatifs à la

---

[210] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), *JORF* n°0020 du 24 janvier 1995 [en ligne] ; LOPSI ; Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, *JORF* n°66 du 19 mars 2003 [en ligne] ; LOPPSI.

[211] Voir principalement : CSI ; Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*

[212] DURAND (F.), « La notion de « La notion de sécurité intérieure à travers les livres blancs et le code de la sécurité intérieure », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 239-252, spéc. p. 245.

[213] CSI, art. L. 242-6.

[214] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 936.

sécurité et la doctrine, qui l'excluent, d'autre part[215]. Les termes de « sécurité publique » semblent par conséquent s'imposer à cette étude des drones aériens introduits comme outils de support aux activités des agents des forces de l'ordre et des sapeurs-pompiers.

Section 4 Le rapport entre sûreté et sécurité à l'aune des drones aériens « augmentés » de sécurité publique

74. Le recours aux drones aériens « augmentés » de sécurité publique est déjà d'actualité. Dès lors, ils s'insèrent présentement dans le rapport sûreté-sécurité. Pourtant, le législateur tarde à mettre en œuvre un cadre juridique en adéquation avec les enjeux qu'ils présentent pour les droits et libertés notamment quant aux atteintes qu'ils sont susceptibles de porter au droit à la sûreté (§1). L'étude portera sur l'introduction du concept de sécurité dans le droit français et sur sa matérialisation par les technologies « augmentées » (§2).

§1. Enjeux de la recherche

75. Depuis plusieurs années, les évènements à caractère terroriste et la multiplication des actes de violence (ex. agressions physiques ou verbales ou encore attaques cybercriminelles) constituent le socle du développement d'une politique sécuritaire privilégiant des valeurs de sauvegarde de l'ordre public souvent au détriment des droits et libertés des individus. La quête perpétuelle du pouvoir politique national d'accroître les mesures sécuritaires tend à renforcer la fragilisation des fondations sur lesquelles repose le système juridique français. Aussi, face aux différentes situations susceptibles de mettre en péril les individus et la nation, les autorités publiques ont développé une certaine tendance à recourir de manière systématique aux nouvelles technologies, que certains qualifient de « solutionnisme technologique »[216]. Sous l'effet de la peur[217], qui comme le rappelle René Sève s'avère « assurément mauvaise conseillère »[218], le législateur agit de manière

---

[215] DURAND (F.), « La notion de « La notion de sécurité intérieure à travers les livres blancs et le code de la sécurité intérieure », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 239-252, spéc. p. 251. Voir aussi : CSI, Livre VII relatif à la « sécurité civile ».

[216] MOROZOV (E.), *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique*, Limoges, éditions FYP, 2014, 350 p.

[217] SERRES (M.), « La peur », *France info*, 4 novembre 2012 [en ligne] : En ce sens, Michel Serres déclarait que notre civilisation « fait l'éloge de la sécurité » et que « le terrorisme est une vague fondamentale de peur ».

[218] SÈVE (R.), « Avant-propos : La mesure de l'ordre public », *in* SÈVE (R.), *L'ordre public*, *op. cit.*

irrationnelle en votant des dispositions offrant davantage de marge de manœuvre aux forces de l'ordre renforçant, en contrepartie, les limites portées aux libertés[219].

76. Opportunité pour les uns, menace pour les autres, le recours à des drones aériens divise principalement lorsque ceux-ci sont destinés à une utilisation par les forces de l'ordre. Leur emploi dans un cadre de sécurité publique s'avère d'autant plus controversé lorsqu'ils sont associés à des algorithmes « augmentés » visant à analyser en temps réel ou post-mission les évènements survenant sur la voie et dans les lieux publics. Leurs qualités techniques en font des outils attractifs en faveur d'un renforcement de l'efficacité des activités des forces de l'ordre et des services de secours qui répondrait aux objectifs de sauvegarde de l'ordre public. L'emploi de cette technologie devra néanmoins respecter une condition nécessaire au maintien de l'État de droit que la professeure Mireille Delmas-Marty définissait comme « un État soumis au droit, dans un double sens impliquant les garanties juridiques institutionnelles (séparation des pouvoirs) et substantielles (respect des droits fondamentaux) »[220]. Ainsi, le recours à des outils technologiques dans le cadre des activités de sécurité publique ne devra pas porter une atteinte disproportionnée aux droits et libertés revêtant un caractère fondamental au motif de vouloir répondre aux exigences de l'ordre public.

77. Le rapport entre sûreté et sécurité sera analysé en partant du postulat que la sécurité se veut constituer un moyen de garantir tant les libertés que l'ordre public alors que la sûreté se veut être un moyen de garantir à l'individu l'exercice de ses droits et libertés en s'opposant à l'arbitraire étatique et que l'ordre public constitue un moyen de limiter ces droits et libertés lorsque leur exercice est compromis. Les libertés et l'ordre public sont interdépendants mais ne peuvent coexister au même moment. La sécurité entendrait par conséquent réunir deux objectifs pourtant opposés. Partant de ce postulat, la sûreté et la sécurité ne peuvent coexister, la sécurité venant empiéter sur le champ de la sûreté.

---

[219] De manière non-exhaustive, la législation relative au renseignement et la lutte contre le terrorisme constitue un des exemples les plus explicites à l'image de la Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *JORF* n°0255 du 31 octobre 2017 [en ligne] pérennisée par la Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *JORF* n°0176 du 31 juillet 2021 [en ligne]. De même la législation en matière de vidéoprotection, codifiée dans le CSI, octroie un large champ d'action en matière de surveillance aux forces de l'ordre. Voir aussi : HANICOTTE (R.), « Espace public, impasse des libertés », *JCP A* n° 26, 2 juillet 2012, 2227 ; LATOUR (X.), « Sécurité intérieure : un droit "augmenté" », *AJDA* n° 8, 5 mars 2018, p. 431.

[220] DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », issu du cours « Libertés et sûreté dans un monde dangereux » des 3 et 10 mars 2009 au Collège de France, *op. cit.*, p. 467.

78. D'une manière générale, cette thèse entend analyser l'incidence des drones aériens de sécurité publique dotés d'algorithmes « augmentés » sur les droits et libertés. Cette étude vise à déterminer en quoi les drones aériens « augmentés » de sécurité publique favorisent la transformation de l'approche du droit à la sûreté, issu du droit commun, en faveur d'une sécurité reposant sur des règles d'exception. En d'autres termes, il s'agit d'évaluer dans quelle mesure cette technologie constitue un moyen de pérenniser des règles d'exception visant à répondre aux nouvelles exigences de l'ordre public au détriment des règles de droit commun qui reposent sur un principe de liberté. Aussi, l'objet de cette thèse entend déterminer à quelle forme de délégation appartiennent les algorithmes « augmentés » qui accompagneront les drones aériens de sécurité publique (délégation d'activités de police ou de pouvoirs de police). En outre, l'étude tentera de mesurer en quoi les drones aériens « augmentés » de sécurité publique peuvent être facteurs d'une redéfinition de l'État de droit en France en faisant reposer une part des décisions régaliennes sur les résultats d'un algorithme « augmenté ».

§2. Problématique et plan de l'étude

79. Problématique - L'étude tente de déterminer comment redéfinir et réformer des garanties efficaces pour les droits et libertés, à l'heure où les drones aériens « augmentés » de sécurité publique investissent déjà l'espace aérien national et interrogent le rapport entre sûreté et sécurité. Comment assurer une protection concrète des droits et libertés face aux algorithmes « augmentés » de sécurité publique qui demain entendent analyser les évènements survenant sur la voie publique ? Quels sont les effets potentiels des algorithmes d'analyse d'images issues des drones aériens dans le processus décisionnel des forces de sécurité publique ? Enfin, en quoi l'introduction croissante des technologies de surveillance de l'espace public et la présence grandissante du secteur privé au sein des activités relevant du pouvoir régalien mènent au délitement progressif de l'État de droit ?

80. Plan - Afin de répondre à ces interrogations, il convient d'étudier l'évolution du cadre juridique tenant aux caméras de surveillance et aux algorithmes numériques utilisés à des fins de sécurité publique. L'étude des effets, tant juridiques qu'éthiques, liés à l'introduction des drones aériens « augmentés » de sécurité publique dans un contexte général d'accroissement du nombre des mesures d'exception permet d'obtenir une vue d'ensemble de l'état des lieux du rapport sûreté-sécurité. D'une manière plus générale, il s'agira d'étudier les effets du recours aux technologies

« augmentées » de surveillance par les autorités publiques sur l'État de droit (**Partie 1**).

81. Dans l'objectif d'apporter des solutions concrètes à la protection des droits et libertés, il convient ensuite d'analyser l'évolution des garanties liées au rapport entre la sûreté et la sécurité sous le prisme de l'introduction massives de nouvelles technologies au sein des activités régaliennes. Cette analyse permettra ensuite d'exposer plusieurs éléments de réponse qui reposeront sur les recommandations et lignes directrices ainsi que sur les principes issus du droit commun (**Partie 2**).

Première partie

UNE NOUVELLE APPROCHE DU RAPPORT SÛRETÉ-SÉCURITÉ INDUITE PAR LES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

« *L'adversaire d'une vraie liberté est un désir excessif de sécurité* ».

Jean de La Fontaine, *Le Loup et le Chien*.

82. L'emploi de drones aériens associés à des algorithmes « augmentés » à des fins de sécurité publique se veut être un élément de réponse à la demande croissante d'une partie de la population pour une amélioration des moyens mis en œuvre en faveur d'une sécurisation de la voie publique. Le recours à ces technologies s'inscrit dans la continuité d'un mouvement général visant à renforcer la prévention des atteintes aux personnes et à leurs biens qui s'est accéléré suite aux attaques terroristes de 2015. Les premiers algorithmes de surveillance de l'espace public ont déjà commencé leur œuvre. Les drones aériens offrent, quant à eux, de nouvelles opportunités aux forces de l'ordre et aux services de secours afin d'assurer la sauvegarde de l'ordre public. De manière plus générale, ces technologies participent à un changement de paradigme depuis longtemps observé où le privilège accordé à la sécurité jette une ombre sur la sûreté, renforçant ainsi les contraintes imposées aux droits et libertés (**Titre 1**).

83. L'intérêt autant que les enjeux juridiques des drones aériens de sécurité publique ne reposent pas uniquement sur leur caractère mobile et le nombre de données qu'ils peuvent collecter mais aussi, et peut être principalement, sur les algorithmes auxquels ils peuvent être associés. Ces algorithmes pourraient analyser les données collectées à des fins préventives ou répressives sans aucune garantie de contrôle de leur fonctionnement ni même de leur utilisation par l'État (**Titre 2**).

TITRE I LES CAMÉRAS DE SÉCURITÉ PUBLIQUE DANS LE RAPPORT SÛRETÉ-SÉCURITÉ

84. Le constat d'un accroissement des atteintes à l'ordre public et à la sécurité nationale a conduit les collectivités territoriales à s'équiper, dès les années 1990, d'un réseau de caméras destiné à filmer la voie publique. Le recours à des caméras fixes a permis aux forces de l'ordre d'assurer une plus grande surveillance de l'espace public. Néanmoins, le succès de cette technologie dans le domaine de la sécurité publique mérite d'être nuancé tant en termes d'efficience que d'acceptabilité par les défenseurs des droits et libertés. Ces dernières années, les drones aériens destinés à des activités de sécurité publique ont été présentés comme une nouvelle forme d'outils de surveillance plus adaptés aux différentes missions des agents des forces de l'ordre ainsi que celles des services de secours. Palliant les inconvénients tenant aux caméras fixes filmant la voie publique, les drones aériens introduisent de nouvelles perspectives d'amélioration de la sécurité publique. Toutefois, la volonté de faire évoluer des drones aériens en milieu urbain a nécessité une adaptation de la règlementation aérienne française afin de tenir compte de leurs spécificités (tenant à leurs objectifs et à leurs contraintes) ainsi que des obligations issues des conventions internationales en matière de droit aérien (**Chapitre 1**).

85. Nonobstant les bénéfices que peuvent apporter les drones aériens de sécurité publique, leur objectif de surveillance de la voie publique a rapidement suscité l'inquiétude des défenseurs des droits et libertés. Leur introduction dans l'espace public a donc nécessité la mise en œuvre d'un cadre juridique adapté qui a fait l'objet de nombreux remaniements avant d'être finalement adopté. Cependant, le contrôle attentif du Conseil constitutionnel n'a pas permis à cette législation de répondre à toutes les questions en matière d'application des droits des personnes de manière concrète. De surcroit, les autorités publiques souhaitent avoir recours à des algorithmes afin de traiter, en temps réel, l'importante quantité de données issues de ces drones aériens et potentiellement prévenir les atteintes à l'ordre public. Bien que les technologies associant des algorithmes à des caméras de surveillance de la voie publique (communément appelées « caméras intelligentes ») puissent apporter des solutions en matière de sécurité publique, celles-ci pâtissent d'un manque d'encadrement juridique adapté à ce type d'usages (**Chapitre 2**).

CHAPITRE 1 L'EXPANSION DES CAMÉRAS DE SÉCURITÉ PUBLIQUE

86. Le développement croissant de technologies à l'usage de la sécurité publique constitue l'un des principaux effets des attentats terroristes qui ont atteint différentes parties du globe depuis le 11 septembre 2001. Face aux dangers, la plupart des États démocratiques ont ainsi basculé vers une politique sécuritaire où le numérique joue un rôle prépondérant. Cette politique exigeante incite toujours davantage au renforcement de l'efficacité de la sécurité nationale et de la sécurité publique. Les innovations technologiques se sont alors majoritairement imposées comme sources de solutions.

87. L'introduction des outils numériques dans le champ de la sécurité publique s'est naturellement présentée comme un facteur d'amélioration de l'efficacité des missions des agents. Parmi ces outils, les caméras de surveillance se placent parmi les plus plébiscitées dans les changements apportés à la mise en œuvre des missions de sécurité publique[221]. Ces caméras, lorsqu'elles filment la voie publique, sont regroupées sous le terme de « systèmes de vidéoprotection »[222] qui font depuis longtemps l'objet d'un encadrement législatif. Cependant, leur encadrement et les atouts qu'ils présentent dans la gestion des évènements du quotidien n'ont pas suffi à atténuer la controverse dont ils font l'objet tenant tant aux enjeux juridiques de garantie de l'exercice des droits et libertés qu'à ceux liés à l'effectivité de cette technologie. Face aux critiques remettant en cause l'efficacité des caméras fixes, les drones aériens offrent une nouvelle opportunité d'assurer la surveillance de la voie publique tout en palliant les contraintes auxquelles sont encore confrontées les caméras fixes de vidéoprotection (**Section 1**).

88. Après de nombreuses années passées au service des forces armées, les drones aériens se sont aujourd'hui fait une place parmi les outils au service de la sécurité publique. Les nombreuses qualités et possibilités d'application dont ils disposent leur confèrent une image d'outil indispensable en vue de répondre aux besoins de garantie de l'ordre public exprimés tant par les agents de sécurité publique que par les citoyens. Ils présentent l'intérêt de constituer un support aux activités de prévention et de répression des atteintes à l'ordre public comme à celles de secours aux

---

221 Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*, spéc. pp. 143-144 : « La vidéoprotection, un outil de sécurisation devenu majeur ».

222 V. **n° 96 et suiv.** Terminologie introduite par la Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), *op. cit.* et CSI, Livre II, Titre V.

personnes et de lutte contre les incendies. À cette fin, la France s'est évertuée à développer un cadre juridique aérien à l'usage des drones visant tant à assurer leur intégrité que celle des personnes au sol et de leurs biens (**Section 2**).

Section 1 Une promesse d'amélioration de la sécurité publique par l'intermédiaire des innovations technologiques

89. Le renforcement des exigences de l'ordre public lié à l'augmentation du nombre des infractions recensées, et plus particulièrement des actes terroristes, ont conduit au développement massif du réseau de caméras de surveillance filmant l'espace public. Face à l'expansion de cette technologie, le législateur a dû rapidement intervenir afin de mettre en œuvre une législation déterminant les limites et les garanties à l'exercice des droits et libertés. Nonobstant l'existence de cette législation, les caméras de surveillance de l'espace public pâtissent encore d'une réputation controversée quant à leur effectivité ainsi qu'au sentiment renvoyé d'une surveillance généralisée de la population (§1).

90. Les déboires des caméras fixes assurant la surveillance de la voie publique ont lentement amené les autorités publiques à faire appel à d'autres technologies plus adaptées aux différentes situations auxquelles sont confrontées les forces de l'ordre. Les drones aériens sont apparus comme une technologie prometteuse pour pallier les inconvénients des caméras fixes et offrir des moyens supplémentaires aux agents des forces de l'ordre et des services de secours. Les drones aériens ont dû néanmoins se miniaturiser afin de répondre aux contraintes tenant au milieu urbain pour lequel ils sont destinés à évoluer. Cependant, les industriels ont su rapidement s'adapter à cette demande de miniaturisation tout en conservant les avantages inhérents aux drones aériens. De par leurs nombreux avantages, les drones aériens sont perçus comme des outils numériques particulièrement attrayants aux yeux des forces de l'ordre comme à ceux des services de secours[223] (§2).

§1. Les caméras de sécurité publique : des dispositifs controversés

91. Face aux enjeux juridiques que soulèvent les caméras de surveillance, notamment en considération du droit à la vie privée, le législateur s'est évertué à mettre en œuvre un encadrement

[223] PAUVERT (B.), « L'utilisation des drones à l'appui de la sécurité », *JCP A* n°27, 5 juillet 2021, p. 2220.

de leur installation et de leur utilisation par les acteurs du secteur public (A). L'existence de ce cadre juridique n'a pourtant pas suffi à éloigner les débats entourant cette technologie à de multiples égards[224]. Ces dernières années, les évolutions technologiques dont ont bénéficié les outils de surveillance de la voie publique ont été autant plébiscitées que controversées. Le constat d'une amélioration de la qualité des données collectées et de la gestion des évènements serait contrebalancé par un cadre juridique de plus en plus inadapté souvent renforcé par le constat d'un défaut d'effectivité (B).

A. L'extension de la législation relatives aux caméras de sécurité publique

92. Le recours à des caméras de surveillance[225] filmant les lieux et espaces publics[226] a constitué un tournant dans l'exercice des activités de sécurité publique. Dès le début des années 1990, la France voit apparaitre les premières caméras destinées à filmer la voie publique. Elles ont été introduites dans l'objectif de tranquilliser la population et de prévenir les troubles à l'ordre public[227]. En ce sens, les premiers acteurs ayant mis en œuvre ce dispositif espéraient « que la surveillance mènerait à la constitution d'un réflexe d'auto-contrainte chez les délinquants » et qu'il permettrait dans le même temps « de rassurer les populations face au sentiment d'insécurité montant »[228]. Cette volonté d'assurer la protection des personnes et des biens par les outils de surveillance de la voie publique s'est exprimée autant par les dispositions juridiques que par la

---

224 BAUER (A.) et FREYNET (F.), *Vidéosurveillance et vidéoprotection*, Paris, PUF, coll. Que sais-je ?, 2012, 128 p., p. 3.

225 Le terme de surveillance doit être entendu comme « toute activité qui consiste en l'observation, la collecte, l'enregistrement et le traitement non occasionnel de données à caractère personnel d'une ou de plusieurs personnes relatives à des comportements, des mouvements, des itinéraires et des communications et à l'utilisation d'appareils électroniques ou informatiques » (CEYHAN (A.) (dir.), Étude « Gendarmerie et technologie : l'impact de la haute technologie sur la sécurité. Analyse comparée », *Centre de prospective de la gendarmerie Nationale*, 2005, p. 55).

226 Les lieux et espaces publics (par opposition aux lieux privés) comprennent la voie publique, mais aussi « les bâtiments et installations publics et leurs abords, les installations utiles à la défense nationale, la voirie routière, les installations accueillant du public dans les parcs d'attraction » et tout « lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants » (Circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (décret sur la vidéosurveillance), *JORF* n°285 du 7 décembre 1996 [en ligne]). En substance, la vidéoprotection concerne « les routes, les places publiques, les équipements collectifs, les dépendances accessoires aux biens publics, etc… » (MORNET (M-N.), *La vidéosurveillance et la preuve*, Aix-Marseille, PUAM, Thèse, 2004, 347 p., p. 27). La jurisprudence judiciaire définit pour sa part le lieu public comme « un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions » (TGI de Paris, 23 octobre 1986 position confirmée par un arrêt de la CA de Paris le 19 novembre 1986 [en ligne]).

227 MARCEL (F.), « Les technologies de sécurité dans le code de la sécurité intérieure », p. 124 *in* MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, *op. cit.*

228 CEYHAN (A.) (dir.), Étude « Gendarmerie et technologie : l'impact de la haute technologie sur la sécurité. Analyse comparée », *op. cit.*, p. 58.

terminologie adoptée (1). Par la suite, leur généralisation s'est imposée comme étant un des moyens les plus efficaces pour surveiller et « protéger » la voie publique. La diversification et le développement exponentiel du réseau de caméras de surveillance en France repose ainsi principalement sur une volonté d'assurer une meilleure sécurité des personnes et de leurs biens par une prévention des infractions et la poursuite de leurs auteurs (2).

1. De la vidéosurveillance à la vidéoprotection

93. Aujourd'hui, les caméras filmant la voie publique occupent une place prépondérante dans l'espace public et sont au cœur des activités des forces de l'ordre. Elles ont une double vocation, étant un outil qui se veut être autant préventif que répressif[229]. Elles présentent, de fait, un objectif de dissuasion reposant sur l'entrave à la commission d'une infraction et offrent, dans le même temps, la possibilité d'identifier l'auteur d'une infraction par la collecte d'images pouvant revêtir la qualité de preuve dans le cadre d'un procès pénal. Le recours à des caméras fixes se veut être une réponse aux besoins exprimés par les forces de l'ordre chargées de préserver l'ordre public ainsi qu'à la demande générale de la population en faveur d'une plus grande sécurité de la voie publique[230].

94. L'installation des premiers systèmes de caméras destinés à filmer la voie publique a rapidement suscité l'inquiétude des défenseurs des droits et des libertés de voir apparaître une forme de surveillance massive de la population. Afin de pallier les potentielles dérives liées à une utilisation disproportionnée de ces systèmes et de rassurer les différents acteurs, le législateur a mis en œuvre un cadre spécifique à l'usage des caméras de surveillance. Le recours aux caméras de surveillance filmant la voie publique a fait l'objet d'un premier encadrement par la loi du 21 janvier 1995[231], dite « LOPS », qui conditionne de manière stricte leur recours. Ce cadre juridique fut par la

---

[229] Voir notamment : HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 502 ; DOUILLET (A-C.) et GERMAIN (S.), « Vidéosurveillance : contexte et problématiques », pp. 10-11 *in* DOUILLET (A-C.), GERMAIN (S.), HELLEMAN (É.) et MELCHIOR (P.), *Vidéo-surveillance ou vidéo-protection ?*, Paris, Le Muscadier, coll. Le choc des idées, 2012, 127 p. ; BAUER (A.) et FREYNET (F.), *Vidéosurveillance et vidéoprotection*, *op. cit.* ; MORNET (M-N.), *La vidéosurveillance et la preuve, op. cit.*, p. 16.

[230] OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 404 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 190.

[231] Plus particulièrement l'article 10 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), *op. cit.*

suite complété par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme[232] venue renforcer l'encadrement de ces dispositifs, apporter des précisions quant aux motifs et aux types d'infractions pouvant faire l'objet d'une telle surveillance et élargir le champ d'application à celui de la prévention d'actes terroristes. Le législateur avait ainsi introduit un contrôle préalable imposant l'obtention d'une autorisation du préfet territorialement compétent avant toute installation d'un dispositif filmant la voie publique[233]. Le législateur permet néanmoins des exceptions à l'obligation du contrôle préalable dans des circonstances précisément définies reconnues comme relevant de cas d'urgence[234]. Cette exception a pour seul objectif de s'adapter aux besoins des autorités publiques afin d'avoir la réactivité nécessaire lorsque les circonstances l'exigent[235].

95. Le régime juridique tenant aux caméras de surveillance a fait l'objet d'un approfondissement par la loi du 14 mars 2011[236] dite « LOPPSI »[237]. Cet ensemble législatif entendait concilier les objectifs de sauvegarde de l'ordre public avec les droits et libertés de chacun. À cette fin, les dispositions relatives aux caméras de surveillance se limitent à celles filmant les lieux et espaces publics. Bien que la LOPPSI ait permis de préciser la réglementation applicable aux caméras filmant la voie publique, des reproches ont été fait au législateur de s'être davantage concentré sur les aspects procéduraux plutôt que sur les garanties effectives préservant les droits et libertés[238]. Certains auteurs ont ainsi qualifié cette démarche de mesure d'« administrativisation » du cadre juridique de ces caméras, suggérant que la complexification de la procédure aura suffi à banaliser ce procédé de surveillance au point que celle-ci semble devenir la règle (s'insérant par conséquent dans le droit commun) et non plus l'exception[239]. La révision du cadre juridique

---

[232] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, *JORF* n°0020 du 24 janvier 2006 [en ligne].

[233] CSI, art. L. 252-1.

[234] *Idem* et CSI, art. L. 223-4, L. 223-5, L. 252-6 et L. 252-7.

[235] Voir en ce sens : LATOUR (X.), « La vidéoprotection et les collectivités territoriales » *in* DANTONEL-COR (N.) (dir.), *Les politiques publiques locales de sécurité intérieure*, Paris, L'Harmattan, 2015, 308 p., p. 277.

[236] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), *op. cit.*

[237] Sénat, Rapport d'information n°131 (2008-2009) sur « La vidéosurveillance : pour un nouvel encadrement juridique » présenté par COURTOIS (J-P.) et GAUTHIER (C.), 10 décembre 2008 [en ligne].

[238] Voir en ce sens : OBERDORFF (H.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 408 ; WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 798 ; BENESTY (G.), « Le clair-obscur du contrôle de la vidéosurveillance », *AJDA* n° 14, 19 avril 2010, p. 764, spéc. p. 770.

[239] ROLIN (F.) et SLAMA (S.), « Les libertés dans l'entonnoir de la législation anti-terroriste : Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers », *AJDA* n°18, 15 mai 2006, p. 975.

présentait un intérêt dual en opérant un changement d'ordre sémantique qui substituait au terme de « vidéosurveillance » celui de « vidéoprotection »[240], d'une part, et en renforçant les garanties quant à leur installation et leur utilisation, d'autre part.

96. Le terme de « vidéoprotection » peut être définit comme « toute technique permettant d'assurer la surveillance de bâtiments, installations, biens et personnes par des caméras vidéos transmettant les images filmées sur un écran télévisuel »[241]. Le rapport de la Cour des comptes sur « Les polices municipales » publié en octobre 2020 propose une définition plus spécifique estimant que « toutes les fois que sont mis en œuvre au moins une caméra et un moniteur, c'est-à-dire un écran permettant la visualisation des images »[242] le procédé relève du cadre de la vidéoprotection. Selon elle, toutes caméras fixes ou mobiles filmant la voie publique, fonctionnant ou non en continu, collectant des images de manière séquentielle ou de manière aléatoire, dont les images peuvent être transférées en temps réel ou être visionnées en différé, sur place ou dans un lieu distant entrent dans le cadre de la vidéoprotection[243].

97. L'objectif de cette évolution sémantique reposait sur l'ambition d'adopter une approche sensiblement différente de ces dispositifs de surveillance. Au départ, l'utilisation du terme « surveillance » soulignait une « volonté protectrice et bienveillante qui cherche à éduquer, à corriger et à étudier scientifiquement »[244]. Toutefois, le recours à de nouvelles technologies capables d'enregistrer de nombreuses informations a progressivement terni l'image de la notion de surveillance. Les caméras filmant la voie publique s'inscrivent dans une architecture où les personnes qui observent sont dissimulées derrière les caméras aux yeux des personnes surveillées. Le terme de « surveillance » traduit alors plutôt une volonté de contrôle par l'État favorisant les actions préventives qui restreignent cependant l'exercice des droits et libertés. L'introduction du terme « protection » avait pour vocation d'accentuer cette volonté de préserver la population face aux dangers et par voie de conséquence de présenter une meilleure image des usages de cette

---

[240] LOPPSI, art. 17.

[241] SAINT-PAU (J-C.), « Fasc. 20 : Vidéoprotection », *JCl Lois pénales spéciales*, 21 mars 2016.

[242] Cour des comptes, « Rapport : Les polices municipales », octobre 2020, p. 62 [en ligne].

[243] *Ibid*.

[244] GANASCIA (J-G.), « De la surveillance à la "sousveillance" », p. 125 *in* CHARDEL (P-A.) (dir.), *Politiques sécuritaires et surveillance numérique*, Paris, CNRS Éditions, coll. les essentiels d'Hermès, 2014, 216 p.

technologie par les autorités publiques[245]. En réalité, il ne s'agissait donc que d'un moyen pour les représentants de l'État de détacher l'augmentation du nombre de caméras déployées sur la voie publique de l'effet de surveillance suscité et du renforcement de leur caractère contraignant pour les droits et libertés[246].

98. Le renforcement des règles ayant trait à la vidéoprotection témoigne de l'amplification du phénomène de surveillance par la prolifération des caméras. Le changement de terminologie entendait renvoyer une image plus protectrice (et positive) de ces outils plutôt que celle d'une surveillance de masse. Pour autant, l'accroissement du nombre des caméras filmant l'espace public constitue une forme de priorité donnée à la sécurité (entendue comme moyen de préserver l'ordre public) sur les droits et libertés. La création du Code de la sécurité intérieure[247] (CSI), comprenant les dispositions relatives à la vidéoprotection[248] issues de la LOPPSI, constitue un éminent témoignage de l'installation pérenne de règles d'exception tenant à la sécurité dans le droit commun. Il aura notamment permis d'ancrer la notion de sécurité intérieure dans le droit ne laissant plus de doute sur l'implication croissante que l'État entendait confier aux acteurs issus du secteur privé au sein des missions d'origine régalienne. Le CSI a donc intégré durablement les systèmes de vidéoprotection dans l'arsenal des technologies visant à assurer la sécurité des personnes et des biens. Durant la décennie suivante, d'autres formes de caméras de surveillance de la voie publique ont fait leur apparition incluant notamment les drones aériens de sécurité publique.

2. La diversification des outils de vidéoprotection

99. Compte tenu de la diversité des systèmes de vidéoprotection, des finalités et des capacités sur lesquels ils reposent, leur caractère intrusif et leur efficacité peuvent sensiblement varier. Aussi,

---

[245] CROUZATIER-DURAND (F.), « De la vidéosurveillance à la vidéoprotection, une nouvelle conciliation des exigences de sécurité et de liberté ? : À propos de la circulaire du 28 mars 2011 d'application de la Loppsi 2 relative à la prévention de la délinquance », *JCP A* n°22, 30 mai 2011, 2196 : « ces deux termes ont une acception quelque peu différente : alors que la surveillance suppose le contrôle, la protection quant à elle implique davantage la défense, le soutien ; l'action de préserver contre un éventuel danger ».

[246] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 502 : « Il s'agit là d'une substitution de termes à laquelle l'objectif de paraître moins menaçant pour les libertés n'est certainement pas étranger… » ; TÜRK (A.), *La vie privée en péril, des citoyens sous surveillance*, Paris, Odile Jacob, 2011, 270 p., p. 84 : « en vérité, […] l'appellation "vidéoprotection" s'inscrit dans une stratégie de communication visant à rassurer, à normaliser le développement massif de la vidéosurveillance ».

[247] Le CSI résulte de la mise en œuvre de l'ordonnance n° 2012-351 du 12 mars 2012 relative à la partie législative du code de la sécurité intérieure, *op. cit.*

[248] CSI, art. L. 251-1 et suiv.

différentes institutions ainsi que plusieurs membres de la doctrine appelaient une révision des dispositions en matière de vidéoprotection afin de tenir compte des différentes évolutions du domaine[249] et du niveau d'incidence que présente la caméra sur les droits et libertés. Récemment, le législateur a tenté de répondre à ces attentes par la loi du 25 mai 2021 pour une sécurité globale préservant les libertés[250]. Celle-ci avait notamment pour objectif de mettre en œuvre un cadre législatif plus adapté tenant compte des progrès technologiques dans le domaine de la vidéoprotection. Toutefois, il apparait clairement que l'adoption de cette législation vient surtout répondre aux demandes des autorités publiques exprimées de manière détaillée dans le rapport intitulé « d'un *continuum* de sécurité vers une sécurité globale »[251] et dans le *Livre blanc* sur la sécurité intérieure[252].

100. Cette loi introduit une nouvelle terminologie, celle de la « sécurité globale » qui peut être définie comme « la participation de tous – police nationale, gendarmerie, police municipale, sécurité privée, sécurité dans les transports – à la construction et à la mise en œuvre d'un dispositif où chacun est mobilisé en vue de l'objectif commun [une meilleure sécurité] »[253]. Après avoir étendu le champ des missions de sécurité aux acteurs issus du secteur privé, le législateur vient donc ici réaffirmer sa volonté de promouvoir une co-création de la sécurité de la voie publique par les forces de l'ordre et les acteurs issus du secteur privé. Aussi, le législateur installe durablement le postulat selon lequel l'amélioration des missions de sécurité publique repose pour une grande part sur le recours à la technologie numérique[254]. La loi du 25 mai 2021 démontre ainsi une nouvelle fois la tendance persistante de l'État et des autorités publiques à nourrir de grands espoirs dans les technologies numériques sans pour autant en démontrer l'efficacité réelle[255].

---

[249] Voir notamment : MBONGO (P.), « Forces publiques de sécurité et état de droit », *in* VALLAR (C.) et LATOUR (X.) (dir.), *Le droit de la sécurité et de la défense en 2013*, Aix-Marseille, PUAM, 2014, 334 p., p. 46 ; Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, pp. 72-76 ; CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018 [en ligne].

[250] Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *JORF* n°0120 du 26 mai 2021 [en ligne].

[251] Rapport de la mission Parlementaire, « D'un *continuum* de sécurité vers une sécurité globale » remis par THOUROT (A.) et FAUVERGUE (J-M.), septembre 2018 [en ligne].

[252] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*

[253] AN, Rapport n° 3527 sur la proposition de loi relative à la sécurité globale, 5 novembre 2020 [en ligne].

[254] WARUSFEL (B.), « La place de l'image : caméras et vidéoprotection dans la sécurité globale », *JCP A* n°27, 5 juillet 2021, 2219.

[255] Voir *supra*.

101. La proposition de loi s'était démarquée par la diversité et la sensibilité des questions qu'elle traitait au regard des droits et libertés[256]. Son objet reposait principalement sur deux aspects : un renforcement des pouvoirs de la police municipale et de l'encadrement des acteurs privés exerçant des missions de sécurité pour le compte de l'État, d'une part, et l'élargissement du champ d'application de la vidéoprotection et de la captation d'images par les forces de l'ordre, d'autre part. Dès lors, celle-ci fut lourdement contestée[257] au point d'être qualifiée par certains auteurs de « loi pour la sécurité particulière des policiers »[258] et de faire l'objet d'un film dans lequel plusieurs professeurs de droit viennent décrire et contester ces dispositions qu'ils considèrent comme attentatoires aux droits et libertés[259].

102. Le texte fit l'objet d'un examen préalable de constitutionnalité le 20 mai 2021[260] avant d'être finalement promulgué. De manière générale, le Conseil constitutionnel reprochait au législateur le manque de clarté et de garanties de nombreuses dispositions ne permettant pas de concilier l'équilibre « entre les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions et le droit au respect de la vie privée »[261]. Le texte avait donc été frappé d'inconstitutionnalité partielle, à juste titre, en raison de certaines de ses dispositions (notamment celles relatives à l'utilisation de drones aériens équipés de caméras) qui ne permettaient pas de garantir de manière suffisante les droits et libertés de chacun. Néanmoins, la déclaration d'inconstitutionnalité de nombreuses dispositions du texte n'aura pas empêché cette législation d'entrer dans le droit commun. Le Conseil constitutionnel semble ainsi approuver le législateur quant à la nécessité d'avoir recours aux technologies en vue d'assurer une meilleure sécurité des personnes et des biens. Aussi, cette loi s'inscrit dans la continuité « de ce processus, devenu irréversible, et qui consiste à renforcer la surveillance des personnes et de certains

---

256 COLLET (P.), « La vidéoprotection et la captation d'images dans la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés », *Communication - Commerce électronique* n°9, septembre 2021, p. 14.

257 PARROT (K.), « La proposition de loi sur la « sécurité globale » poursuit subrepticement une transformation sécuritaire de la politique pénale », *op. cit.*

258 ROUSSEAU (D.), « Sécurité globale : une vrai-fausse proposition de loi, une vrai privatisation de la surveillance, des réserves et censures ambigües », *Gaz. Pal.* n°21, 8 juin 2021, p. 19.

259 PARROT (K.) et ELMADJIAN (S.), Film « Sécurité globale, de quel droit ? », *op. cit.*

260 C. const., Décision n° 2021-817 DC, 20 mai 2021, *Loi pour une sécurité globale préservant les libertés, JORF* n°0120 du 26 mai 2021 [en ligne].

261 *Ibid*.

lieux »[262].

103. Cette loi aura toutefois eu le mérite d'introduire de nouvelles garanties au recours à des caméras de vidéoprotection par les forces de l'ordre[263]. En ce sens, le texte insère de nouvelles dispositions relatives aux caméras fixes au sein du CSI, tenant à la formation des agents des forces de l'ordre en matière de protection des données à caractère personnel ainsi qu'aux mesures techniques de sécurité informatique (assurant la sécurité des enregistrements et la traçabilité des accès aux images). Les évènements survenus durant la pandémie impliquant l'usage de drones aériens équipés de caméras par la préfecture de police de Paris ont souligné le cruel manque de maitrise et de considération à l'égard des dispositions relatives à la protection des DACP. Il paraissait, de fait, indispensable de renforcer la maitrise du contenu de cette réglementation par ces agents. En outre, la prolifération des attaques informatiques ayant eu lieu depuis le début de la pandémie en 2020 aura largement contribué à éclairer le besoin primordial de renforcer les mesures à mettre en œuvre en matière de sécurité informatique.

104. Enfin, la loi du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure (RPSI)[264] vient encore étoffer le cadre juridique intéressant le domaine de la vidéoprotection. Elle comprend notamment de nouvelles dispositions concernant les caméras de surveillance installées ou intégrées sur des aéronefs en vue de filmer la voie publique. La loi, examinée par le Conseil constitutionnel lors de sa décision du 20 janvier 2022[265], permet l'introduction d'un cadre strict des nouveaux dispositifs de vidéoprotection au sein du CSI ainsi que du Code de procédure pénale (CPP). Ces nouveaux dispositifs que sont les drones aériens (désignés par la loi sous les termes de « caméras aéroportées ») et les caméras embarquées (installées sur des avions ou des hélicoptères) peuvent désormais être utilisés dans le cadre de missions relevant de la police administrative autant que de la police judiciaire. Toutefois, le Conseil constitutionnel a tenu à limiter l'usage des drones aériens à des fins de sécurité publique aux seuls agents exerçant au sein

---

[262] COLLET (P.), « La validité contestable de la vidéosurveillance de la voie publique en enquête préliminaire », *JCP G* n° 26, 28 juin 2021, act. 711.

[263] Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*, art. 40, et CSI, art. L. 255-1.

[264] Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure (RPSI), *op. cit.*, art. 15 et 16.

[265] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, *JORF* n°0020 du 25 janvier 2022 [en ligne].

de la police et de la gendarmerie nationales excluant ainsi les agents de la police municipale[266]. Les Sages ont estimé que les dispositions en matière de recours à ces dispositifs par les membres de la police municipale méconnaissaient le droit au respect de la vie privée.

105. La loi pour une sécurité globale préservant les libertés du 25 mai 2021 et la loi relative à la responsabilité pénale et la sécurité intérieure du 24 janvier 2022 affichent clairement cette volonté des pouvoirs publics de systématiser le recours aux technologies en vue d'améliorer la sécurité publique. Les défenseurs des droits et libertés évoquent parfois une forme de « solutionnisme technologique »[267] qui consiste à recourir de manière presque systématique à des moyens technologiques supposés répondre de manière concrète aux problèmes que l'être humain seul n'est pas en mesure de résoudre. Ainsi, les technologies transforment voire déforment le droit en le soumettant à leurs exigences. Le professeur Bertrand Warusfel dénonce en ce sens une mobilisation de la norme de droit non plus « pour produire par elle-même un effet mais pour définir les conditions dans lesquelles un outil technique va pouvoir être mis en œuvre pour parvenir au résultat poursuivi »[268]. Dès lors, la norme juridique ne serait plus celle qui adapte les moyens au droit commun afin de répondre aux besoins en matière de sécurité publique et serait à l'inverse contrainte de s'adapter aux moyens, en l'occurrence technologiques, au point d'être réduite à la simple fonction de protection contre les potentiels litiges opposant l'État à sa population.

106. En outre, les innovations technologiques, bien que porteuses de nombreuses opportunités d'amélioration de la sécurité publique, ne sont pas pour autant irréprochables. Elles font encore l'objet de nombreuses contestations quant à leur efficacité concrète compte tenu de l'incidence qu'elles ont sur l'exercice des droits et libertés tels que la liberté d'aller et venir ou encore le droit de manifestation.

---

[266] *Idem*, cons. 35-37.

[267] Voir notamment : CNIL, « La CNIL rend son avis sur la proposition de loi "sécurité globale" », 3 février 2021 [en ligne] ; WARUSFEL (B.), « La place de l'image : caméras et vidéoprotection dans la sécurité globale », *op. cit.* ; CLUZEL-MÉTAYER (L.), « les aspects numériques de la loi pour la sécurité globale ou l'avènement de la "technosurveillance globale" », p. 103 *in* GALLOIS (J.) et MUREL (R.) (dir.), *La sécurité globale. Perspectives juridiques & éthiques*, Paris, L'Épilogue, coll. L'unité du droit, 2022, 190 p. ; Syndicat de la magistrature, « Observations du Syndicat de la magistrature sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure - Volet n°3 : dispositions relatives à la surveillance (Articles 7, 8, 9) », 21 septembre 2021 [en ligne]. Sur le « solutionnisme technologique » : MOROZOV (E.), *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique*, *op. cit.*

[268] WARUSFEL (B.), « La place de l'image : caméras et vidéoprotection dans la sécurité globale », *op. cit.*

B. Le recours contestable aux caméras de sécurité publique

107. Les caméras fixes de vidéoprotection offrent encore aujourd'hui une certaine capacité de dissuasion. Pour autant, leur efficacité réelle quant à prévenir et réprimer les infractions est souvent remise en question[269] (1). En ce sens, certains auteurs évoquaient « l'effet plumeau » de ces caméras de vidéoprotection ; en d'autres termes un déplacement des lieux où se déroulent les infractions du fait de la présence de ces caméras. Nonobstant les progrès technologiques dont elles bénéficient désormais, ces caméras présentent encore des freins techniques liés à leur caractère statique qui ne leur permet pas de visualiser l'entièreté des événements. Par ailleurs, outre les enjeux relatifs à son efficacité, cette technologie présente un coût qui ne semble pas toujours être justifié au vu du manque d'informations relatives à l'évaluation de l'efficacité des dispositifs de vidéoprotection (2).

1. L'efficacité relative de la vidéoprotection

108. Ces quinze dernières années, le nombre des dispositifs de vidéoprotection a sensiblement augmenté[270]. Le ministère de l'Intérieur estimait à environ 27 000 le nombre des caméras dans tout l'espace public français en 2009 et prévoyait un nombre total de 60 000 pour 2012[271]. Néanmoins, dans son rapport de 2011, la Cour des comptes ne comptabilisait qu'environ 10 000 caméras de surveillance filmant la voie publique fin 2010[272]. En 2012, la CNIL délivrait une estimation encore bien différente en recensant 70 003 caméras installées sur la voie publique et 827 000 dans différents lieux ouverts au public[273]. Dans son rapport d'octobre 2020[274], la Cour des comptes

---

269 Voir notamment : COURMONT (A.) et SALIOU (J.), « Comment la vidéosurveillance vient au village ? », *linc.cnil.fr*, 19 novembre 2021 [en ligne] consulté le 13 janvier 2023 ; LEMAIRE (É.), *L'oeil sécuritaire : Mythes et réalités de la vidéosurveillance*, Paris, La Découverte, 2019, 208 p. ; MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, Malakoff, Armand Collin, 2018, 222 p. ; GORMAND (G.), *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier*, Université Grenoble Alpes, Thèse, 2017 ; DOUILLET (A-C.), GERMAIN (S.), HELLEMAN (É.) et MELCHIOR (P.), *Vidéo-surveillance ou vidéo-protection ?*, *op. cit.* ; MARCEL (F.), « Les technologies de sécurité dans le code de la sécurité intérieure », pp. 124-125 *in* MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, *op. cit.*

270 MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, *op. cit.*, spéc. pp. 25-32.

271 AN, Rapport d'information sur « la contribution de l'État au développement de la vidéoprotection » présenté par GEOFFROY (G.), 13 juillet 2010, 33 p. [en ligne]

272 Cour des Comptes, « Rapport public thématique : L'organisation et la gestion des forces de sécurité publique », 7 juillet 2011 [en ligne].

273 CNIL, « Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », 21 juin 2012 [en ligne].

274 Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 64.

évaluait, cette fois, entre 60 674 et 76 457 le nombre de dispositifs de vidéoprotection[275]. Ce nombre ne tenait toutefois compte que des caméras fixes (excluant les dispositifs de vidéoprotection mobiles tels que les caméras individuelles portées par les agents lors des missions ou encore les drones aériens destinés à la sécurité publique). Ces écarts de comptabilisation pourraient s'expliquer par la différence entre le nombre de caméras ayant fait l'objet d'une autorisation et celui des caméras effectivement installées. Les services du ministère de l'Intérieur recenseraient le nombre de caméras installées par celui des caméras autorisées ; or, il arrive que seul certains systèmes de vidéoprotection soient véritablement installés[276].

109. L'accroissement du nombre de caméras met en lumière tant l'usage exponentiel d'outils technologiques par les forces de l'ordre au sein de l'espace public que la généralisation du recours à l'expertise de chercheurs issus des milieux scientifiques mais également des ingénieurs commerciaux[277]. Les nombreux projets pluridisciplinaires (financés par les différents organismes nationaux comme supranationaux dédiés à la recherche), associant des partenaires issus du secteur tant privé que public afin de développer des outils d'assistance aux missions de sécurité publique, en sont indiscutablement des témoins. Aussi, les progrès technologiques ont favorisé cette appétence des forces de l'ordre pour les caméras de surveillance par les bénéfices qu'elles présentent. Les avancées technologiques ont permis d'améliorer les performances en matière de surveillance de l'espace public, qu'il s'agisse de la qualité des données pouvant être collectées ou encore du traitement automatisé de celles-ci.

110. Bien que la généralisation des systèmes de vidéoprotection ait désormais pris une place prépondérante au sein des politiques de sécurité, celle-ci n'a jamais cessé de faire l'objet de controverses, qu'il s'agisse de son efficacité ou de son coût. En France, les caméras de surveillance filmant la voie publique font encore l'objet d'un débat animé. Aujourd'hui, les critiques portent davantage sur les progrès technologiques dont elles bénéficient, ayant à la fois pour conséquence d'accroître leur efficacité mais également leur pouvoir contraignant pour les droits et libertés. En

---

[275] En 2018, la Direction générale de la police nationale dénombrait 37 757 caméras (hors Paris) et la Direction générale de la gendarmerie nationale comptabilisait 38 700 caméras soit un total de 76 457 caméras tandis que « de son côté, la DLPAJ dénombrait 60 674 caméras installées au 31 décembre 2018, soit 16 000 caméras de moins que celles comptabilisées par les forces de sécurité, sans que cette statistique ait pu recevoir une explication » (Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 64).

[276] DOUILLET (A-C.), GERMAIN (S.), HELLEMAN (É.) et MELCHIOR (P.), *Vidéo-surveillance ou vidéo-protection ?*, *op. cit.*, p. 9.

[277] LAVENUE (J-J.) et VILLABA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, *op. cit.*, p. 10.

outre, le débat s'est élargi aux nouvelles formes de caméras (individuelles, drones, embarquées sur des aéronefs)[278] qui, compte tenu de leur miniaturisation et de leur caractère mobile, interrogent la concrétisation d'une conciliation entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public, d'une part, et les droits inhérents à la vie privée et au procès pénal, d'autre part. Au cœur de ce débat réside la question essentielle de leur efficacité face aux attentes et aux contraintes qu'elles engendrent pour la population.

111. Depuis son apparition dans l'espace public, la vidéoprotection suscite autant d'enthousiasme que de méfiance. Les défenseurs de la vidéoprotection perçoivent ces outils comme un moyen d'assurer la sécurité, la sûreté et l'exécution des procédures particulières[279] et considèrent ces caméras comme étant des « instruments essentiels à la prévention et à la répression des actes terroristes »[280]. En ce sens, l'Institut national des hautes études sur la sécurité et la justice (INHESJ) considère la vidéoprotection comme cruciale à la mise en œuvre de la sécurité publique et reconnaissait que même « si les effets de la vidéoprotection ne sont pas toujours mesurables en termes de baisse de la délinquance, le sentiment d'insécurité est toujours favorablement impacté »[281]. Cette affirmation dénote cependant une propension dangereuse à favoriser un effet placebo des dispositifs de vidéoprotection par une contrainte - réelle- pour les droits et libertés des personnes circulant sur la voie publique. Pourtant, aux yeux de leurs défenseurs, les systèmes de vidéoprotection ne constitueraient non pas une menace à l'exercice des droits et des libertés mais seraient *a contrario* un vecteur garantissant leur protection. L'objectif des outils de vidéoprotection repose ainsi principalement sur la prévention des atteintes à l'ordre public en suscitant un effet de dissuasion des potentiels auteurs d'infractions afin de rassurer la population. Dans un rapport d'inspection concernant l'efficacité de la vidéoprotection du 1er juillet 2009[282], les forces de l'ordre ont confirmé l'utilité de ces dispositifs lors des missions tant de maintien de l'ordre (actions de

---

[278] CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018 [en ligne].

[279] LAVENUE (J-J.) et VILLABA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, *op. cit.*

[280] CROUZATIER-DURAND (F.), « De la vidéosurveillance à la vidéoprotection, une nouvelle conciliation des exigences de sécurité et de liberté ? : À propos de la circulaire du 28 mars 2011 d'application de la Loppsi 2 relative à la prévention de la délinquance », *op. cit.*

[281] INHESJ, « La vidéo-protection. Conditions d'efficacité et critères d'évaluation », *IHEMI*, 2008 [en ligne].

[282] Ministère de l'Intérieur, « Rapport sur l'efficacité de la vidéoprotection » émis par SALLAZ (J-P.), DEBROSSE (P.) et HAN (D.), 1er juillet 2009, 82 p. [en ligne].

prévention) qu'à des fins d'investigation judiciaire (actions répressives).

112. À l'inverse, les opposants à la vidéoprotection lui reprochent un manque d'efficacité face à la petite délinquance, qu'elle ne ferait que déplacer (d'où l'appellation du phénomène d'« effet plumeau »)[283]. Le caractère fixe de la plupart des systèmes de vidéoprotection restreint considérablement leurs capacités dissuasives laissant toujours le constat d'un simple déplacement des zones où sont commises les infractions. En ce sens, Jean Ruegg évoquait les caméras fixes de vidéoprotection comme des outils visant « moins à discipliner les comportements des individus qu'à discipliner des territoires [et par conséquent] à rendre certains quartiers ou secteurs plus sûrs … parfois aux dépens d'autres »[284]. Elles entraineraient par voie de conséquence des formes d'inégalités de la sauvegarde de l'ordre public entre les individus sur tout le territoire.

113. En France, cette méfiance persistante à l'égard de la vidéoprotection pourrait s'expliquer à deux égards. D'une part, l'insuffisance nette du nombre d'études statistiques et d'évaluations indépendantes françaises effectuées concernant leur efficacité concrète ne permet pas de gagner la confiance des opposants à la vidéoprotection. D'autre part, les statistiques font encore état de résultats assez marginaux de l'efficacité des caméras fixes de vidéoprotection[285] y compris au Royaume-Uni, qui pourtant profite d'un des plus importants réseaux de caméras de surveillance d'Europe.

2. L'insuffisante démonstration d'efficacité confrontée aux coûts de la vidéoprotection

114. Aujourd'hui encore, les systèmes de vidéoprotection pâtissent d'une insuffisance nette de démonstration de leur efficacité qui résulte d'un manque d'études des effets obtenus dans le cadre des missions des forces de l'ordre[286] (a). Cette absence de justification du recours aux outils de

---

283 MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, *op. cit.*, spéc. pp. 127-151 ; COURMONT (A.) et SALIOU (J.), « Comment la vidéosurveillance vient au village ? », *op. cit.*

284 RUEGG (J.) (dir), Rapport « Vidéosurveillance et risques dans l'espace à usage public - Représentations des risques, régulation sociale et liberté de mouvement », CETEL, Université de Genève et de Fribourg, octobre 2006, p. 236.

285 Voir en ce sens : FROMENT (J-C.), « Regard juridique sur la vidéosurveillance urbaine : un droit en trompe-l'œil », *JCP A* n° 13, 27 mars 2006, pp. 435-440 ; LE GOFF (T.), « La vidéosurveillance est-elle une réponse efficace à la délinquance ? », *AJP* n° 6, 11 juin 2010, p. 275.

286 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 38 : « Le déploiement de la vidéoprotection n'avait pas fait l'objet d'une évaluation approfondie sur les effets, en termes de prévention de la délinquance et d'aide aux enquêtes ».

vidéoprotection se confronte aux coûts engendrés par ces technologies que la Cour des comptes a eu l'occasion de souligner (b).

a. L'absence d'évaluations concrètes de l'efficacité de la vidéoprotection

115. Le recours à la vidéoprotection est soumise à un principe de proportionnalité exigeant la démonstration de la nécessité de faire usage de ces dispositifs[287]. L'acceptabilité de ces caméras par les différents acteurs nécessite par conséquent l'apport d'une démonstration de leur efficacité tant s'agissant de leurs finalités dissuasives que répressives. Sur ce sujet, la Cour des comptes se place parmi les premières institutions à se préoccuper et à contribuer à l'information de ces usages par la publication de ses rapports publics[288]. D'après les conclusions de son enquête issues de son rapport de 2020, elle estime que l'efficacité des caméras fixes de surveillance de la voie publique n'a pas été démontrée. Les rapporteurs ont estimé qu' « aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de délinquance commis sur la voie publique »[289].

116. En plus d'une vingtaine d'années d'exploitation, les systèmes de vidéoprotection n'auront fait l'objet que d'un seul rapport public évaluant leur efficacité (rapport précité). C'est sous la pression des critiques suscitées par l'absence d'évaluation des dispositifs de vidéoprotection que le gouvernement a enjoint, en 2009, les inspections générales de l'administration, de la police et de la gendarmerie nationales de rendre ce rapport. Il aura d'ailleurs fait l'objet d'une analyse par deux chercheurs critiquant vivement tant le processus d'évaluation que la fiabilité de son contenu[290]. Dans leur étude, Tanguy Le Goff et Éric Heilmann dénonçaient principalement le manque de rigueur de la part des inspections générales, qui n'avaient pas respecté les règles mises

---

[287] Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 70 : « La vidéoprotection peut être parfois l'objet de recours en contentieux » où les juges peuvent apprécier, en fonction du lieu, le caractère proportionné ou non de l'installation d'une ou de plusieurs caméras « au regard des nécessités de l'ordre public ». En outre, « la CNIL, rappelle régulièrement qu'une évaluation de la nécessité et de la proportionnalité du dispositif envisagé, au regard des finalités poursuivies, doit être opérée avant son implantation ».

[288] MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, *op. cit.*, spéc. pp. 97-98 ; HAYEZ (P.), « La Cour des comptes : du contrôle à l'évaluation », *Revue française d'Administration publique* n°3, 2015, pp. 707-711 ; PRAT (M-P.) et JANVIER (C.), « La Cour des comptes auxiliaire de la démocratie », *Pouvoirs* n° 3, 2010 pp. 97-107.

[289] Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, pp. 69-71.

[290] LE GOFF (T.) et HEILMANN (É.), « Vidéosurveillance : un rapport qui ne prouve rien », *Délinquance, justice et société*, 24 septembre 2009 [en ligne] consulté le 16 janvier 2023.

en œuvre par les évaluations internationales en matière de caméras surveillant la voie publique[291]. Le rapport ne permettait pas par conséquent d'affirmer avec certitude que ces dispositifs constituaient un moyen effectif de prévention de la commission d'infractions. Aussi, ils avaient constaté que le rapport minimisait le déplacement de la délinquance (« effet plumeau ») par l'installation de caméras fixes filmant la voie publique. Pourtant, les deux chercheurs soulignaient que cette « question [était] systématiquement abordée dans les études évaluatives étrangères » et que celles-ci « mettent en évidence que les déplacements de la délinquance ne sont pas systématiques [et] dépendent du type de délits et d'espaces sur lesquels opèrent les caméras de surveillance »[292].

117. Encore aujourd'hui, les études françaises analysant l'efficacité de la vidéoprotection reposent sur des travaux de recherches sociologiques. Celles-ci formulent des conclusions similaires quant au manque d'efficacité concrète des systèmes de vidéoprotection. Les travaux de recherche de Guillaume Gormand comprennent ainsi une étude détaillée des évaluations menées en France et à l'étranger des dispositifs de vidéoprotection. Ses recherches lui ont permis de formuler plusieurs constatations[293]. Il observe qu' « il est très exceptionnel que les images captées par la vidéosurveillance à l'occasion du suivi d'une intervention mettent en lumière la commission d'infractions »[294]. Aussi, il constate que « même dans des études retenues comme démontrant un effet avéré de la vidéosurveillance comme outil de prévention situationnelle de la délinquance, les chercheurs révèlent en réalité que son caractère dissuasif se trouve être largement surestimé »[295]. Dans le même sens, Laurent Mucchielli dénonçait que « non seulement la vidéosurveillance de rue

---

[291] Voir notamment : NORRIS (C.) et MORAN (J.), "Evaluating the effectiveness of CCTV schemes", pp. 16-19 *in* NORRIS (C.) et MORAN (J.), *Surveillance, Closed Circuit Television and Social Control,* London, Routledge Edition, 1998, 304 p. ; PIZA (E), WELSH (B.), FARRINGTON (D.) and THOMAS (A.), "CCTV surveillance for crime prevention : A 40-year systematic review with meta-analysis", *Criminology & Public Policy* 18(1), March 24th 2019, pp. 135-159 [en ligne] ; GILL (M.) and FISCHER (P.), "Does CCTV displace crime ?", *Criminology and Criminal Justice* n°2, vol. 9, 2009, pp. 207-224 [en ligne] ; WELSH (B.) and FARRINGTON (D.), "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis", *Justice Quarterly* n° 26, October 12th 2009, pp. 716-745 [en ligne] ; FARRINGTON (D.), GILL (M.), WAPLES (S.) et ARGOMANIZ (G.), "The effects of closed-circuit television on crime: meta-analysis of an English national quasi-experimental multi-site evaluation", *Journal of Experimental Criminology* n° 3, 2007, pp. 21-38 [en ligne].

[292] LE GOFF (T.) et HEILMANN (É.), « Vidéosurveillance : un rapport qui ne prouve rien », *op. cit.*, pp. 2-3.

[293] GORMAND (G.), *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier*, *op. cit.*, pp. 97-142.

[294] *Idem*, p. 319.

[295] *Ibid*. Voir également : HEILMANN (É.), « La vidéosurveillance, une réponse efficace à la criminalité ? », *Criminologie*, vol. 1, 2003, pp. 89-102 ; LE GOFF (T.) et FONTENEAU (M.), « Vidéosurveillance et espaces publics, État des lieux des évaluations menées en France et à l'étranger », IAU-RIF, Paris, 1er octobre 2008 [en ligne] ; WELSH (B.) and FARRINGTON (D.), "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis", *op. cit.*

n'est pas particulièrement efficace dans la lutte contre la délinquance mais elle n'est pas fondamentalement utilisable et utilisée dans ce but »[296]. Aussi, ses recherches lui ont permis d'affirmer qu'il n'était pas possible d'évaluer précisément l'incidence préventive de ces dispositifs sur la population (délinquante ou non)[297]. Enfin, Élodie Lemaire constatait qu'en matière de preuve dans le cadre d'une procédure judiciaire le recours aux images issues des caméras fixes de vidéoprotection s'avérait assez complexe et qu'elles n'étaient pas nécessairement décisives dans le traitement de l'affaire[298].

118. Aussi, l'efficacité des systèmes de vidéoprotection s'évalue selon le type de caméras mis en œuvre. De fait, les caméras fixes ne bénéficient pas du même retour que les caméras individuelles. Aujourd'hui, les caméras fixes pâtissent encore de nombreuses limites sur le plan technologique suscitant l'insatisfaction de leurs utilisateurs (ex. manque de visibilité, de précision, de netteté, de taille de l'image, etc.). Néanmoins, de nombreux progrès technologiques dans le domaine de la surveillance ont déjà permis de pallier certaines limites auxquelles faisaient face les caméras fixes tant sur le plan technique (ex. rotation de la caméra à 360 degrés, amélioration de la qualité des images, etc.) que sur le plan technologique (ex. nombre et types de données collectées, amélioration du flux vidéo, introduction d'algorithmes de comptage et de détection d'individus ou d'objets, etc.).

119. Face à l'absence du nombre d'études gouvernementales sur ce sujet, la Cour des comptes a pris l'initiative de mener son enquête afin d'évaluer le niveau d'efficacité des systèmes de vidéoprotection. Les résultats, issus de son analyse de l'échantillon de son enquête portée au niveau local, lui ont permis d'affirmer qu' « aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation »[299]. Aussi, la Cour des comptes fait même état d'une augmentation du contentieux en matière de vidéoprotection suite au déploiement de ces dispositifs. D'une manière générale, les juges estiment que la vidéoprotection se justifie dans certains lieux. Toutefois, ils observent que l'augmentation du nombre de caméras est perçue comme étant « disproportionnée au

---

[296] MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, *op. cit.*, pp. 175-176 ; MUCCHIELLI (L.), « À quoi sert la vidéosurveillance ? », *VST* n°154, février 2022, pp. 23-29, spéc. 28 [en ligne].

[297] MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, *op. cit.*, p. 176.

[298] LEMAIRE (É.), *L'oeil sécuritaire : Mythes et réalités de la vidéosurveillance*, *op. cit.*, pp. 137-165.

[299] Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 70 et annexe n°9 Statistiques de la délinquance, service statistique ministériel de la sécurité intérieure.

regard des nécessitées de l'ordre public »[300]. Sur ce sujet, la CNIL souligne l'importance que revêt l'obligation préalable d'évaluation de la nécessité et de la proportionnalité du dispositif en accord avec les finalités poursuivies à l'installation de tout dispositif de vidéoprotection[301].

120. Dans son rapport de 2020, la Cour des comptes rappelait que les études d'impact portant sur les systèmes de vidéoprotection ont longtemps reposé sur une base d'études étrangères. Celles-ci faisaient apparaitre deux principaux constats, celui d'une variabilité des résultats selon le type de lieu et celui d'une variabilité selon le type d'infraction[302]. Dès lors, ces études concluaient que les systèmes de vidéoprotection s'avèreraient peu efficaces dans les espaces ouverts et complexes. En revanche, toutes les études faisaient état d'une réelle efficacité de ces systèmes dans les espaces fermés (ex. bâtiments ou parkings). Dans son étude comparative avec d'autres États européens, la Cour des comptes avait fait le constat qu'en Allemagne le nombre de caméras installées dans les lieux publics demeurait assez faible[303] et se limitait essentiellement aux gares ou à certains quartiers à haut taux de délinquance[304]. Elle observe notamment que le déploiement de dispositifs de vidéoprotection dans les Länder s'effectue principalement lors d'évènements importants et note que « en 2018, lors de la fête de la bière de Munich, le nombre de caméras de surveillance est passé de 38 à 47 »[305].

121. Cette analyse permet d'émettre l'hypothèse selon laquelle l'efficacité des caméras fixes de vidéoprotection serait davantage démontrée lors de grands événements et qu'elle ne se s'apprécie pas par le nombre de caméras placées mais davantage par le lieu de leur installation. Ainsi, le recours à des caméras fixes de vidéoprotection se justifierait plutôt à l'occasion de grands évènements d'ordre festif ou sportif (ex. dans des stades ou salles de concert) qu'à des fins de surveillance permanente de la voie publique. Il conviendrait alors de faire usage d'autres outils de vidéoprotection dans le cadre des missions quotidiennes de maintien de l'ordre public et de police

---

300 *Idem*, p. 70.

301 CNIL, « La vidéosurveillance – vidéoprotection sur la voie publique », 3 décembre 2019 [en ligne] et CNIL, Délibération n°2021-078 du 8 juillet 2021 portant avis sur un projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, avis n° 21012005, p. 3 [en ligne].

302 LE GOFF (T.), « La vidéosurveillance est-elle une réponse efficace à la délinquance ? », *op. cit.*

303 D'après la Cour des comptes, la rigueur de la Loi fondamentale allemande protégeant la vie privée des citoyens pourrait être à l'origine de cette faible présence des caméras fixes.

304 Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 152 (annexe n°5 Le déploiement de la vidéoprotection en Europe).

305 *Ibid*.

judiciaire. Pour autant, les caméras fixes demeurent l'outil le plus fréquent employé à des fins de vidéoprotection, engendrant des coûts qui sans évaluation d'efficacité s'avèrent de plus en plus difficile à justifier.

122. Dix ans après son premier rapport sur la vidéoprotection, la Cour des comptes a fustigé une nouvelle fois ses usages estimant que son efficacité n'était que rarement démontrée et ce en dépit des coûts importants qu'elle engendre[306]. Elle estimait que compte tenu de banalisation de l'utilisation de la vidéoprotection et de l'étendue de son déploiement « il est peu concevable qu'aucune réflexion ne soit engagée quant à son efficacité »[307]. En outre, elle soulignait l'inadéquation voire l'absence d'encadrement juridique à l'égard de certaines formes de vidéoprotection telles que les caméras dites « intelligentes » ayant recours à des formes de technologies avancées en matière d'IA mais aussi les drones aériens dont les forces de l'ordre faisaient déjà usage[308]. Elle reformule ainsi sa recommandation de 2011 enjoignant le ministère de l'Intérieur « d'engager une évaluation de l'efficacité de la vidéoprotection de la voie publique, notamment dans l'élucidation des crimes et délits, avec le concours de chercheurs et d'experts (SGMI, DCS, DACG) »[309]. Néanmoins, elle constatait avec satisfaction que plusieurs de ses recommandations en matière de vidéoprotection formulées en 2011, avaient conduit à la mise en œuvre de comités de suivi et d'évaluation de ces dispositifs dans différentes communes.

b. Les coûts injustifiés de la vidéoprotection

123. La contestation persistante de l'efficacité de la vidéoprotection associée au coût de cette technologie soulèvent naturellement la question de son efficience. Le coût de la vidéoprotection demeure une question centrale de la politique de sécurité et constitue *de facto* un élément essentiel de son processus d'acceptation par la population. La Cour des comptes avait donc entrepris de faire un état des lieux de cette technologie et a mené une étude faisant l'objet d'une analyse détaillée dans son rapport d'octobre 2020[310]. Elle émet le constat que nonobstant la diminution du prix des

---

306 LECHENET (A.), « La vidéosurveillance dans le viseur de la Cour des comptes », *La Gazette des communes*, 26 octobre 2020 [en ligne] consulté le 28 décembre 2022.

307 Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 76.

308 *Idem*, pp. 72-76.

309 *Idem*, p. 77.

310 *Idem*, p. 152.

caméras celles-ci présentaient encore un coût élevé. Cela ne semble pas surprenant étant donné le fait que le nombre de ces dispositifs ne cesse d'augmenter depuis leur apparition au sein de l'espace public[311]. Pour autant, les politiques de sécurité locale semblent avoir davantage privilégié la qualité sur la quantité[312]. Néanmoins, cette qualité a un coût lié « à l'installation, à la maintenance et à l'exploitation de la vidéoprotection »[313].

124. Aussi, la Cour des comptes déplore que peu de communes aient été en mesure de justifier les coûts d'exploitation. En outre, elle s'étonne du fait que, dans de nombreuses communes, les forces de police et de gendarmerie nationales ne reçoivent pas de manière automatique les images issues des caméras de vidéoprotection, alors qu'elles devraient en être les principales bénéficiaires, celles-ci étant plus légitimes que ne le sont les polices municipales s'agissant d'interpeller en flagrance. La Cour des comptes estime, par conséquent, que le financement de ces dispositifs « devrait être conditionné à la possibilité de déport d'images »[314].

125. En 2021, la Cour des comptes avait renouvelé de vives critiques à l'encontre des systèmes de vidéoprotection de la ville de Paris constatant que leur efficacité ne faisait toujours l'objet d'aucune évaluation[315]. Elle constatait que le plan de vidéoprotection de la ville de Paris avait sensiblement changé depuis les attentats de 2015. Face à la menace d'attaques terroristes, la ville de Paris avait bénéficié de crédits alloués notamment à son plan de vidéoprotection lui permettant de tripler le nombre de ses caméras en vue d'améliorer ses capacités de réaction face aux dangers[316]. Pourtant, l'expérimentation croissante des technologies de traitement automatique des flux vidéos par la préfecture de police (ex. vidéo-verbalisation semi-automatique de la circulation sur les voies de bus) ne répondaient pas toujours aux attentes des opérationnels. Aussi, la Cour des comptes avait souligné un manque d'éléments probants dans l'évaluation et le suivi de l'expérimentation de ces technologies ne permettant pas « de lever les freins réglementaires,

---

311 Selon le rapport de la Cour des comptes de 2020, le nombre de caméras de vidéoprotection sur le territoire aurait été multiplié par 6,5 en l'espace d'une décennie.

312 *Idem*, p. 66.

313 *Idem*, p. 67.

314 *Idem*, p. 68.

315 Cour des comptes, Référé S2021-2194 « Le plan de vidéoprotection de la préfecture de police de Paris » adressé au Ministère de l'Intérieur, 2 décembre 2021 [en ligne].

316 *Idem*, p. 2.

financiers et opérationnels qui les limitent »[317]. Dès lors, elle avait formulé des recommandations similaires à celles de son rapport de 2020 qui invitaient le préfet de police de Paris à engager dans les plus brefs délais une évaluation de l'efficacité de son plan de vidéoprotection dans la prévention de la délinquance et l'élucidation des délits[318].

126. Compte tenu du caractère particulièrement intrusif des systèmes de vidéoprotection, de leur coût et de l'amplification du nombre des caméras filmant la voie publique, il parait essentiel que l'évaluation de l'efficacité de ces dispositifs soit davantage prise en considération. Il est surtout inquiétant d'observer que les autorités publiques préfèrent privilégier une fuite en avant technologique censée résoudre les questions liées à la sauvegarde de l'ordre publique afin de rassurer la population au détriment de l'exercice de leurs droits et libertés. Outre l'absence d'évaluation de leur efficacité, il semblerait que les usages de dispositifs de vidéoprotection ne se prêtent pas à toutes les finalités que la législation leur a attribuées. Aussi, l'efficacité de la vidéoprotection pourrait sensiblement dépendre du type de dispositif utilisé. Les contraintes que subissent encore les caméras fixes démontrent l'intérêt d'avoir recours à d'autres types de dispositifs. Néanmoins, il convient de rester vigilant afin de ne pas basculer dans un régime de surveillance permanente de la voie publique. Face aux nombreux écueils des caméras fixes de vidéoprotection, les drones aériens équipés de caméras se sont donc présentés comme une technologie convaincante pour un usage destiné aux activités de sécurité publique tant en termes d'efficacité qu'en termes de coûts.

§2. Les drones aériens de sécurité publique : une réponse aux besoins opérationnels

127. Les innovations technologiques ont largement investi les activités de sécurité publique et présentent des avantages non négligeables en venant en support des agents. Cependant, les avantages procurés par ces technologies engendrent un effet d'amplification de l'exigence d'efficacité des activités dans lesquelles elles sont employées. La facilitation des tâches induites par l'utilisation des innovations technologiques entraine davantage d'attentes quant aux résultats escomptés, allant jusqu'à donner l'impression de ne plus laisser de place à l'erreur ou à l'échec. Il s'ensuit une escalade des exigences attendues dans chaque secteur d'activité et plus

[317] *Idem*, p. 5.

[318] *Idem*, p. 6.

particulièrement en matière de sécurité publique[319]. Ces attentes s'expliquent majoritairement par les attaques terroristes qui ont sévi aux quatre coins du monde. Les demandes en la matière sont larges allant de la lutte contre les attaques à caractère terroriste et la criminalité organisée en passant par celles tenant à la sécurité routière, ou encore la lutte contre les incendies et le secours aux personnes. Les besoins s'expriment également de la part des agents en charge d'assurer la sécurité des personnes et des biens. La diversité des missions (sécurité du quotidien, police judiciaire, gestion de crise, etc.) et des terrains (milieux urbains, périurbains, ruraux, etc.) sur lesquels évoluent les membres des forces de l'ordre nécessite l'appui de nombreux outils technologiques et une adaptation constante de leurs évolutions[320].

128. Aux dires du ministère de l'Intérieur, les drones aériens sont « largement plébiscités par les forces de sécurité intérieure pour leur facilité d'utilisation [et] constituent une capacité à part entière déjà bien développée ou en cours de déploiement (255 drones détenus par la gendarmerie, 235 drones au sein de la police nationale) »[321]. Sans pour autant céder à l'effet de popularité du drone, les forces de sécurité publique ont depuis longtemps identifié des besoins auxquels les drones aériens sont susceptibles de répondre, soit par leur apport opérationnel soit comme moyen alternatif à d'autres outils[322]. Bien que les drones aériens de sécurité publique nécessitent toujours la présence d'un être humain, ceux-ci présentent d'ores et déjà de nombreux avantages. Ils sont à la fois un gage d'efficacité opérationnelle, de sécurité quant à leur usage, de flexibilité d'emploi et de rentabilité[323] (A).

129. La gendarmerie nationale avait ainsi relevé plusieurs qualités du drone aérien compatibles avec la diversité de ses missions telles que sa complémentarité avec d'autres aéronefs

---

319 Voir en ce sens : BALMOND (L.), « Brèves remarques sur la problématique des rapports entre la sécurité et le droit », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2022 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, vol. 7, 2022, 316 p., pp. 283-294, spéc. pp. 291-292 : « la société, pour la très grande majorité de ses membres, a été progressivement habituée à une diminution de l'insécurité celle-ci pouvant provenir aussi bien de l'action des pouvoirs publics nationaux que de la coopération internationale. Cet immense progrès, toutefois très inégalement partagé, a conduit à une exigence constamment accrue de sécurité, notamment face aux "nouvelles menaces" ».

320 Voir à ce sujet : MOREL (J-F.), « Face aux drones, l'approche responsable de la gendarmerie nationale », pp. 259-276 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

321 Ministère de l'intérieur, « Livre blanc de la sécurité intérieure », *op. cit.*, p. 231.

322 *Idem*, p. 261 ; VIDAL (L.), « L'usage en matière de sécurité intérieure des appareils autonomes ou dirigés à distance », pp. 47-55 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

323 Ministère de l'intérieur, « Livre blanc de la sécurité intérieure », *op. cit.*, pp. 268-269.

(ex. hélicoptères), sa capacité d'accélération de l'acquisition des informations par les agents commandant les missions ou encore ses potentialités de renforcement de la protection des personnes au sol[324]. À cela s'ajoute la discrétion, la hauteur de vol, le renforcement de la précision des images et les possibilités de transmission des données en temps réel par le drone aérien[325]. Il parait évident que les drones aériens concentrent de nombreuses qualités pour les agents des forces de l'ordre et les services de secours tant sur le plan opérationnel que du point de vue technologique. Aussi, le drone aérien se démarque par la grande diversité de ses usages potentiels : surveillance à des fins préventives allant des infrastructures essentielles au fonctionnement de l'État (opérateurs d'importance vitale) aux rassemblements de grande ampleur, à la poursuite d'individus suspects, à la reconstruction en trois dimensions d'un bâtiment en flammes, etc[326]. Les drones aériens de sécurité publique offrent des opportunités sommes toutes assez similaires à celles des drones aériens utilisés à des fins militaires[327] (B).

A. Les drones aériens, une technologie « révolutionnaire » pour la sécurité publique

130. Les drones aériens sont reconnus pour leur caractère furtif[328] qui peut reposer sur différents critères tels que leur taille, leur mode de propulsion ou encore leur faculté d'évoluer à des niveaux les rendant presque indétectables[329]. Contrairement aux hélicoptères, les drones aériens disposent de facilités de déploiement[330]. Il ne s'agit bien évidemment pas de facilités administratives de déploiement mais bien de potentialités d'observation. La miniaturisation des drones aériens les rend, de fait, plus maniables, plus discrets et leur offre la possibilité d'évoluer

---

[324] *Ibid*.

[325] WARUSFEL (B.) et BAUDE (F.), *Annuaire 2018 du Droit de la Sécurité et de la Défense*, Lyon, Mare & Martin, Volume 3, 2018, 434 p, p. 160 ; VIDAL (L.), « L'usage en matière de sécurité intérieure des appareils autonomes ou dirigés à distance », p. 48 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

[326] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 39.

[327] WARUSFEL (B.) et BAUDE (F.), *Annuaire 2018 du Droit de la Sécurité et de la Défense*, *op. cit.*, pp. 159 à 163.

[328] MOREL (J-F.), « Face aux drones, l'approche responsable de la gendarmerie nationale », p. 268. *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

[329] EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*, p. 3.

[330] CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 98.

dans des endroits autrement difficiles d'accès, ceux-ci étant en mesure de franchir des obstacles[331] tels qu'un mur ou une barrière. Il va sans dire que du fait de leur petite taille (en comparaison d'autres aéronefs) les drones aériens présentent l'avantage de pouvoir être déployés facilement en n'importe quel lieu et pourront s'exonérer des contraintes de devoir décoller d'un aérodrome.

131. Les drones aériens de sécurité publique sont équipés de caméras et peuvent comprendre également d'autres capteurs[332] leur permettant, d'une part, de palier les inconvénients présentés par les systèmes de vidéoprotection fixes, et d'autre part, de collecter davantage de données avec la possibilité de les transmettre en temps réel au centre de commandement. Outre la collecte d'images, les drones aériens de sécurité publique peuvent répondre à divers autres besoins opérationnels[333]. Aussi, contrairement aux hélicoptères (qui peuvent également être équipés de caméras) les drones aériens offrent une meilleure perception des évènements puisqu'ils peuvent s'approcher de la scène à observer et bénéficier d'un angle de vue plus précis sur la situation en cours[334]. Ils sont un gage de proximité par rapport aux évènements en facilitant la détection et en permettant d'isoler le ou les individu(s) à l'origine d'un trouble à l'ordre public. Cette proximité offre une meilleure qualité des images dans le sens où celles-ci sont focalisées sur l'évènement en question[335], palliant ainsi les désagréments d'un trop grand nombre de données inutiles. En outre, la possibilité de choisir l'angle de prise de vue permet de réduire le risque d'erreur d'interprétation des situations rencontrées.

132. Le nombre et la qualité des données qu'ils peuvent transmettre constitue une source d'information qui peut s'avérer capitale dans le cadre de l'exercice des missions des forces de l'ordre et des services de secours. De fait, la collecte de données constitue « une finalité essentielle

---

331 VIDAL (L.), « L'usage en matière de sécurité intérieure des appareils autonomes ou dirigés à distance », p. 48 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

332 CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 31.

333 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 39 : Ils sont notamment en mesure de « transporter une lampe afin d'éclairer une opération, un haut-parleur afin d'informer une population, une charge d'eau dans un incendie, des équipements de survie pour une personne blessée difficilement accessible, un capteur thermique pour [détecter la présence d'] une personne [en péril] ou un fugitif, des dispositifs de communication radio de secours ». Voir aussi : CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 35.

334 VIDAL (L.), « L'usage en matière de sécurité intérieure des appareils autonomes ou dirigés à distance », p. 48 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.* ; MASSET (C.), « Gendarmerie du transport aérien : réglementation de l'utilisation des drones aériens », p. 170 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

335 CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 98.

de l'action policière »[336]. Une information éclairée des agents permet d'améliorer leur pouvoir d'action lors des missions[337]. Elle offre également une certaine garantie de l'intégrité des agents qui, agissant en pleine connaissance de la situation en cours, sont en mesure de prévenir les actions portées à leur encontre. Dès lors, la vie des agents des forces de l'ordre et des services de secours repose pour une grande part sur la quantité d'informations dont ils disposent. Aussi, la multiplicité des capteurs qui composent les drones aériens leur permet d'effectuer plusieurs tâches en simultané. Ils sont notamment en mesure, grâce à leurs nombreux capteurs, de localiser un individu à l'aide d'un équipement GPS (système de positionnement global), de détecter la présence de personnes ou d'objets dissimulés via des rayons infrarouges, ou encore d'évaluer la température d'une pièce dans le cadre d'un incendie[338]. Ils offrent ainsi un flux permanent d'informations en temps réel des évènements avec l'avantage de cibler les évènements et les lieux les plus pertinents lors des missions. Ce sont ces qualités qui expliquent les raisons pour lesquelles la majeure partie des informations acquises ces dernières années par les agents des forces de l'ordre et des services de secours proviennent de manière significative et croissante des outils de hautes technologies.

133. Certes, il va de soi qu'en termes d'efficacité en temps réel les drones aériens de sécurité publique (à l'instar d'autres outils de vidéoprotection) ne sont pas en mesure d'interpeler un individu en train de commettre une infraction, contrairement à un agent des forces de l'ordre sur le terrain. Cette contrainte, particulièrement s'agissant des atteintes portées à l'encontre de personnes, leur a valu d'être considérés par certains auteurs comme « impropres à des missions de police »[339]. Néanmoins, il parait nécessaire de remettre l'outil dans son contexte. Le recours à des drones aériens de sécurité publique n'a pas pour objectif d'interpeller des individus mais seulement de constituer un support aux agents dans leurs missions.

134. Aussi, à l'inverse des caméras fixes, les agents au centre de commandement qui observeront les images renvoyées par les drones aériens seront en liaison directe avec des agents sur

---

336 EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *RDP* n°1, 1er janvier 2018, p. 189.

337 CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 32 : « En cas de catastrophe ou de crise, la collecte d'informations opérée par les drones peut contribuer à améliorer la connaissance de la situation » (Traduit de l'anglais).

338 VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 54 : « Les drones sont en effet équipés de caméras, de géolocalisation, de capteurs thermiques, de microphones et d'appareils photos, et sont donc des indicateurs indispensables pour les forces de l'ordre » et les services de secours.

339 WARUSFEL (B.) et BAUDE (F.), *Annuaire 2018 du Droit de la Sécurité et de la Défense*, *op. cit.*, p. 161.

le terrain qui seront en mesure d'agir rapidement. Les drones aériens pourraient donc être un gage d'efficacité des activités de sécurité publique en ciblant les évènements les plus pertinents voire même en isolant l'auteur d'une infraction. En outre, les données collectées (principalement des images) par les drones permettront d'effectuer une évaluation *a posteriori* des décisions prises ou de la situation dans son ensemble.

135. Les drones aériens de sécurité publique confèrent des avantages économiques en engendrant de faibles coûts de fonctionnement. À l'inverse des caméras fixes de vidéoprotection, ils ne fonctionnent pas en continu, ce qui réduira les coûts de leur utilisation. Ils s'adaptent aux contraintes budgétaires des forces de sécurité publique en assurant certaines missions qui autrement ne pourraient pas ou difficilement être assurées faute de revêtir un caractère d'urgence absolue nécessitant l'utilisation d'autres moyens aéronautiques (avec un déploiement plus coûteux) ou d'engendrer des difficultés d'ordre technique ou opérationnel[340]. L'usage des drones par les forces publiques présente par conséquent une réelle opportunité d'amélioration de la sécurité publique.

136. Ce sont ces nombreuses qualités, déjà identifiées s'agissant des drones militaires, qui ont conduit les pouvoirs publics à doter les forces de sécurité publique en drones, leur conférant de nouvelles missions relevant de la protection de l'ordre public. Aussi, les capacités dont peuvent faire preuve les drones aériens n'ont pas échappé aux agents de sécurité publique. Cette appétence pour les drones aériens a participé à l'élaboration de nombreux projets dont un projet (financé par l'Agence nationale de la recherche) intitulé « COOPOL » (Capacité d'appui aux Opérations de secOurs et POLice) visait à mettre à disposition des sapeurs-pompiers, des forces de police et de gendarmerie nationales un système multi-drones de secours et d'aide au maintien de l'ordre en milieu urbain[341]. Aujourd'hui, les drones semblent apparaitre comme un outil indispensable à l'exercice des activités relevant de la sécurité publique.

B. Les drones aériens, une technologie adaptée à la sécurité publique

137. Les systèmes de vidéoprotection sont autant une démonstration de l'amplification de la présence des innovations technologiques dans le quotidien qu'un nouvel outil au service des forces

---

340 MOREL (J-F.), « Face aux drones, l'approche responsable de la gendarmerie nationale », p. 261 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

341 cf. Annexe 2.

de l'ordre allant dans le sens de la politique sécuritaire. L'introduction de ces technologies à l'usage des forces de l'ordre et des services de secours participe également aux actions menées en vue de sécuriser les conditions de travail d'une grande part des agents de la fonction publique. Certains métiers du secteur public sont de fait particulièrement exposés à des dangers.

138. Le ministère de l'Intérieur se trouve, sans surprise, être l'un des domaines les plus « accidentogène » du secteur public[342]. Les agents de la police et de gendarmerie nationales sont particulièrement exposés au danger lors des missions. Des statistiques[343] révèlent même une augmentation du nombre des décès ainsi qu'un grand nombre de blessés au sein des membres des forces de l'ordre qu'il s'agisse de missions à caractère préventif ou de missions visant à constater, poursuivre ou réprimer une infraction (caractère répressif). De même, les agents des services d'incendies et de secours sont aussi indéniablement concernés. Plusieurs dispositions ont été mises en œuvre afin d'assurer la santé et la sécurité du travail des agents de la fonction publique. Le décret du 28 mai 1982 relatif à l'hygiène, la sécurité et la prévention médicale à l'ensemble des administrations de l'État[344] ainsi que des dispositions du Code du travail[345] comprennent des obligations opposables à l'État favorisant la sécurité des agents. Parmi les nombreuses obligations techniques de sécurité se trouvent notamment les équipements de travail et de protection ou encore les équipements utiles à la prévention d'expositions aux dangers[346]. La notion de sécurité peut alors

---

342 COLIN (F.), « La sécurité au travail dans la fonction publique », p. 254-255 *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.* En employant le terme « accidentogène » Frédéric Colin fait référence aux accidents du travail dans le domaine de la fonction publique comprenant tant les accidents de service que les maladies professionnelles (ex. blessures, décès, etc.).

343 Sur l'augmentation nette du nombre de blessés et de décès au sein des forces de l'ordre entre 2014 et 2018 : Observatoire national de la délinquance et des réponses pénales, Note n°39 sur « Les policiers et gendarmes décédés et blessés en 2018 » par SOULLEZ (C.), novembre 2019 [en ligne] ; MAINGUET (M.), « Combien de policiers et de gendarmes tués en mission en France ? », *Ouest-France*, 11 mai 2021 [en ligne] ; « Le nombre de policiers et gendarmes blessés en mission a augmenté de 15 % en 2018 », *Le Monde*, 7 novembre 2019 [en ligne].
Sur le nombre de policiers blessés entre 2004 et 2014 : AN, Rapport n° 2678 sur la proposition de loi relative à la légitime défense des policiers remis par CIOTTI (É.) le 25 mars 2015 [en ligne].

344 Décret n° 82-453 du 28 mai 1982 relatif à l'hygiène et à la sécurité du travail ainsi qu'à la prévention médicale dans la fonction publique, *JORF* du 30 mai 1982 [en ligne].

345 Code du travail, 4e partie, Livres 1-5 : Principe et démarche de prévention, règles particulières.

346 COLIN (F.), « La sécurité au travail dans la fonction publique », pp. 256-257 *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*

être assimilée, dans ce cas, à une obligation d'assurer l'intégrité physique par le respect des principes généraux de prévention à l'égard des agents chargés d'assurer la sécurité publique[347].

139. Paradoxalement, l'institution policière est souvent perçue comme privilégiée au sein de la fonction publique[348]. Pourtant, un rapport parlementaire datant de 2018 mettait en lumière un mal-être des forces de l'ordre[349] reposant sur de multiples facteurs parmi lesquels une augmentation des activités opérationnelles et de la pression sécuritaire, conséquence des exigences de sécurité toujours plus prégnantes de la population. Une autre explication retenue par le rapport est celle de l'insuffisance de moyens alloués aux forces de l'ordre leur permettant d'assurer leurs missions dans des conditions satisfaisantes et de faire face aux difficultés induites par une organisation et des méthodes de management largement inadaptées. Le professeur Olivier Cahn souligne, en ce sens, que la révision des politiques publiques a eu pour conséquence de réduire drastiquement les effectifs des forces de l'ordre tout en requérant dans le même temps une augmentation exponentielle de leurs activités (suite aux attaques terroristes et à l'augmentation des mouvements de manifestation)[350]. Faisant face aux contraintes budgétaires et aux exigences formulées par la population en faveur d'une plus grande sécurité des personnes et de leurs biens, l'État a souvent eu recours aux technologies numériques.

140. Les outils numériques de surveillance et d'analyse des évènements constituent des moyens de prévenir les atteintes à l'intégrité physique des agents de la fonction publique. Ils permettent une préparation des missions afin d'identifier les zones de potentiels dangers ainsi que des moyens d'agir pendant les missions afin d'isoler les agents d'une menace à laquelle ils ne sont pas en mesure de faire face de manière immédiate. Le Sénat soulignait également en ce sens que les

---

347 En référence à l'article L. 4121-2 du Code du travail. Voir en ce sens : Circulaire du 10 avril 2015 relative à la diffusion du guide juridique d'application des dispositions du décret n°82-453 du 28 mai 1982 modifié relatif à l'hygiène et à la sécurité du travail, ainsi qu'à la prévention médicale dans la fonction publique [en ligne] ; Circulaire du 28 mars 2017 relative au plan d'action pluriannuel pour une meilleure prise en compte de la santé et de la sécurité au travail dans la fonction publique [en ligne] ; Plan santé au travail dans la fonction publique, 18 mars 2022 [en ligne].

348 Voir notamment : AN, Rapport n°2111 fait au nom de la Commission d'enquête sur la situation, les missions et les moyens des forces de sécurité, qu'il s'agisse de la police nationale, de la gendarmerie ou de la police municipale, rapporté par AEGELEN (C.), 3 juillet 2019, spec. annexe 2 [en ligne] ; « Les policiers obtiennent une revalorisation salariale après une journée de protestation », *Journal du Dimanche*, 20 décembre 2018 [en ligne] ; « Les syndicats de policiers obtiennent une revalorisation salariale », *ladepeche.fr*, 20 décembre 2018 [en ligne] ; « Fronde des policiers : un accord de revalorisation salariale a été conclu entre Castaner et les syndicats », *europe1.fr*, 20 décembre 2018 [en ligne] consultés le 3 janvier 2023.

349 Sénat, Rapport n°612 fait au nom de la commission d'enquête intitulé « Vaincre le malaise des forces de sécurité intérieure : une exigence républicaine », déposé par GROSDIDIER (F.), 27 juin 2018 [en ligne].

350 CAHN (O.), « Un État de (la) police », *RSC* n°4, octobre-décembre 2019, pp. 975-996 spéc. p. 991.

technologies de captation d'images, notamment par drones aériens, « se révèlent particulièrement efficaces dans la lutte contre la délinquance comme pour le maintien de l'ordre, en limitant notamment les contacts des forces de l'ordre avec les personnes concernées »[351]. De manière non négligeable, le pilotage à distance des drones aériens offre l'opportunité de limiter les risques encourus par les agents qui seront isolés de la zone de danger lors des missions, qu'il s'agisse de lutte contre les incendies comme de la gestion d'un évènement tel qu'une émeute. L'évaluation de la zone de mission (et notamment les zones situées en milieu isolé) représente une garantie de préservation de l'intégrité physique des agents sur le terrain, qui disposeront des informations en temps réel[352].

141. Ce gage d'intégrité physique permet de répondre aux obligations de sécurité de l'État vis-à-vis de ses agents. Les drones aériens de sécurité publique constituent par conséquent une amélioration des conditions de travail ainsi que d'efficacité des missions. Cette minimisation des risques encourus est un élément essentiel au processus d'acceptabilité du recours aux drones aériens au sein de l'espace public, tant pour les agents eux-mêmes que pour la population. Dès lors, les drones aériens permettent de pallier les contraintes budgétaires et de venir en support des agents afin qu'ils se tiennent informés des évènements en cours tout en préservant leur intégrité physique.

142. Dans la perspective de satisfaire les besoins exprimés par les agents, plusieurs textes réglementaires ont été mis en œuvre afin d'encadrer l'utilisation des drones aériens au sein de l'espace public. Cette réglementation est rapidement devenue nécessaire en vue de préserver tant l'intégrité physique des personnes au sol que celle des aéronefs évoluant au sein de l'espace aérien national. Elle vient encadrer les pratiques liées à l'usage des drones et s'est progressivement adaptée à chaque forme d'utilisation, allant du domaine militaire vers le domaine professionnel et même de loisirs. Au-delà des dispositions juridiques relatives au survol du territoire par ces aéronefs, la réglementation prévoit désormais une procédure rigoureuse de formation des télépilotes permettant une professionnalisation des acteurs du domaine (v. n° **166-167**).

---

[351] CE, Avis n° 401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, 20 septembre 2020, p. 1 [en ligne].

[352] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 54 : « En observant depuis les airs, [le drone aérien] permet de limiter les risques d'exposition des agents de police [et de secours] et d'épargner ainsi des vies humaines ».

Section 2 Les règles aériennes intégrant les drones dans l'espace urbain à des fins de sécurité publique

143. Le nombre d'aéronefs occupant l'espace aérien a considérablement augmenté et ceux-ci exercent des missions de différentes natures impliquant des règles distinctes[353]. Face à cette situation, il est apparu comme primordial de mettre en œuvre des règles de compatibilité entre les différents usages afin d'assurer la sécurité de tous les usagers et des personnes au sol[354]. L'apparition des drones aériens, particulièrement ceux évoluant au sein de l'espace aérien national, venant encore amplifier le phénomène, a nécessité une adaptation des règles en matière d'aéronautique tant militaire que civile. Les dispositions en matière d'utilisation de l'espace aérien étant souvent inconnues du grand public, les drones aériens ont suscité quelques craintes quant à la manière de les insérer au sein des règles issues du droit aérien. Les drones aériens utilisés à des fins de sécurité publique ont, de fait, la particularité d'être destinés à évoluer au sein de l'espace aérien général[355], faisant apparaitre deux risques potentiels à savoir des collisions avec les autres usagers de l'espace aérien français, d'une part, et, les dommages causés sur les individus survolés, d'autre part. Il s'avérait par conséquent indispensable d'établir un cadre réglementaire de la circulation aérienne intégrant ce type d'aéronefs afin d'assurer l'intégrité physique de tous[356].

144. Introduction des drones aériens en milieu urbain - La règlementation aérienne française scinde l'espace aérien national entre la circulation aérienne générale et la circulation aérienne militaire[357]. Le ministre chargé de l'aviation civile est compétent concernant le domaine de la circulation aérienne générale tandis que la circulation aérienne militaire relève de la compétence

---

353 BROCAREL (A.), « L'insertion et la circulation des drones militaires dans les espaces nationaux », p. 87 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit*.

354 En 2018, le Colonel Laurent Legoff témoignait en ce sens que « la gendarmerie nationale était confrontée à la montée en puissance des drones et à leur prolifération dans le monde civil, mais également au sein de l'institution où plusieurs unités commençaient à s'en doter de manière non maitrisée » cité par MOREL (J-F.), « Face aux drones, l'approche responsable de la gendarmerie nationale », p. 261 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

355 L'espace aérien général doit s'entendre de l'espace utilisé habituellement par les aéronefs civils.

356 Dans un souci d'assurer la sécurité des personnes au sol et des autres aéronefs survolant le territoire national, les forces de l'ordre et les services de sécurité civile s'étaient dotés d'une doctrine d'emploi de leurs drones aériens : l'Instruction 94000/GEND/DOE/SDSPSR/BSRFMS du 1er juillet 2019 relative à l'emploi des systèmes de drone au sein de la gendarmerie nationale ; l'Instruction du 27 juillet 2018 relative à l'emploi des aéronefs télépilotés dans la police nationale ; le document de la préfecture de police relatif aux consignes permanentes opérationnelles s'agissant des drones ; la note de doctrine générale du 11 juillet 2017 relative à l'emploi d'aéronefs télépilotés pour des missions de sécurité civile ; la note de service du 6 mai 2020 relative à la mise en place d'une expérimentation de l'emploi opérationnel des aéronefs télépilotés de la brigade de sapeurs-pompiers de Paris.

357 CAC, art. D.131-2.

du ministre de la Défense[358]. Ces deux types de circulation aérienne reposent sur des règles différentes qui doivent néanmoins être compatibles afin que l'espace aérien puisse accueillir ces types d'usages. À cette fin, la règlementation prévoit que les deux ministres concernés « fixent conjointement les règles qui assurent [leur] compatibilité »[359]. Les deux corps de règles, fixés par décret ou arrêté, sont détaillés de manière précise et comprennent de nombreuses obligations à l'attention de l'exploitant et de ses télépilotes.

145. En droit aérien, les drones à destination des forces de l'ordre et des services de secours sont désignés sous les termes d' « aéronefs sans pilote à bord » et appartiennent à la catégorie des aéronefs militaires et d'État. Toutefois, le fait de recourir à des aéronefs militaires et d'État en milieu urbain complexifie la détermination du cadre réglementaire qui leur est applicable. En ce sens, l'emploi en milieu urbain nécessite l'application d'autres dispositions juridiques que celles issues des textes strictement relatifs aux aéronefs militaires et d'État. Le caractère militaire et d'État des drones de sécurité publique et les modalités de leur introduction dans l'espace aérien national reposent sur un *corpus* législatif et règlementaire très précis issu du droit aérien français ainsi que sur des dispositions générales issues du droit aérien international et européen. L'appréhension du *corpus* de règles tenant aux drones aériens de sécurité publique nécessite d'étudier au préalable la distinction entre les dispositions régissant les aéronefs civils et celles tenant aux aéronefs militaires et d'État, d'une part, et, les dispositions spécifiques relatives aux aéronefs sans pilote à bord.

146. Droit aérien international - Le cadre juridique des drones aériens s'est avant tout construit au sein de la règlementation supranationale avec une première convention internationale sur la navigation aérienne du 13 octobre 1919[360] qui régulait les aéronefs sans pilote. Par la suite, la Convention de Chicago relative à l'aviation civile internationale du 7 décembre 1944[361] (Convention de Chicago) est venue remplacer la convention de 1919[362] tout en conservant des dispositions en matière d'aéronefs sans pilote à bord. Ce texte de référence en matière de droit international de l'aviation établit un cadre réglementaire unifié concernant l'accès et le survol du

---

[358] *Idem*.

[359] BROCAREL (A.), « L'insertion et la circulation des drones militaires dans les espaces nationaux », p. 88 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit*.

[360] Convention de Paris relative à l'aviation civile, 13 octobre 1919, L.N.T.Ser 99 ; 11 L.N.T.S 173 [en ligne].

[361] Organisation de l'aviation civile internationale (OACI), Convention relative à l'aviation civile internationale, Chicago, 7 décembre 1944, 61 Stat, 1180, 15 U.N.T.S 295 ; Doc 7300/9, neuvième édition, 2006, 51 p. [en ligne].

[362] *Idem*, art. 15.

territoire de chaque État, et créée l'Organisation de l'Aviation Civile Internationale (OACI). La Convention dispose d'un champ d'application précis qui exprime clairement la volonté de la communauté internationale de respecter le principe de souveraineté des États[363] et d'exclure les aéronefs militaires et d'État de la réglementation aéronautique internationale[364].

147. L'exclusion des aéronefs militaires et d'État du champ d'application de la Convention se comprend aisément compte tenu du fait que leurs activités militaires sont une expression évidente de l'exercice de souveraineté d'un État sur son territoire. Elle s'explique également par le fait qu'il revient logiquement à chaque État de prendre les décisions qui relèvent des activités de son armée et notamment des risques qu'elle encoure selon le type de missions. Il existe par conséquent deux *corpus* de règles aéronautiques : la règlementation aéronautique civile, établie au niveau international, et une règlementation aéronautique spécifique à chaque État afin de régir les aéronefs d'État. Cette distinction entre l'aéronautique civile et l'aéronautique militaire repose sur les finalités d'utilisation ainsi que sur la relation aux risques d'un aéronef : l'aviation civile tendant à prévenir toute forme de risques pour ses usagers tandis que l'aviation militaire comprend une approche des risques bien différente. La Convention de Chicago ne définit pas ce qu'elle entend par « aéronef civil ». En s'appuyant sur son article 3 énonçant que « les aéronefs utilisés dans des services militaires, de douane ou de police sont considérés comme aéronefs d'État »[365], il est possible d'en déduire que tout aéronef non reconnu comme revêtant la qualité d'aéronef d'État sera considéré comme appartenant à la catégorie des « aéronefs civils » et entrera dans le champ de la Convention.

148. L'exclusion des aéronefs militaires et d'État du champ de la réglementation aérienne supranationale ne les dispense pas néanmoins du respect de certaines règles communes aux aéronefs civils tenant à la sécurité aérienne. La Convention de Chicago mentionne effectivement une obligation d'engagement des États signataires de faire respecter à leur aviation militaire les dispositifs de sûreté et de sécurité applicables à l'aviation civile énonçant que « les États contractants s'engagent à tenir dûment compte de la sécurité de la navigation des aéronefs civils

---

[363] Convention de Chicago du 7 décembre 1944, *op. cit.*, art. 1er. : « Les États contractants reconnaissent que chaque État a la souveraineté complète et exclusive sur l'espace aérien au-dessus de son territoire » qu'elle définit par ailleurs à l'article 2.

[364] *Idem.*, art. 3 (a) : « La présente Convention s'applique uniquement aux aéronefs civils et ne s'applique pas aux aéronefs d'État ».

[365] *Idem*, art. 3 b).

lorsqu'ils établissent des règlements pour leurs aéronefs d'État »[366]. Les aéronefs militaires et d'État doivent par conséquent respecter un *corpus* de règles générales établies par la Convention de Chicago afin d'intégrer l'espace aérien national. Cet encadrement de la liberté des États concernant l'introduction des aéronefs traduit la volonté de ceux-ci d'unifier les règles applicables en matière d'aviation et de sécurité. En d'autres termes, la Convention rappelle que toute disposition que les États signataires mettraient en œuvre afin d'encadrer le vol d'aéronefs au sein de leur espace aérien devra rester conforme à celles issues du traité[367].

149. Droit aérien européen - À l'instar de la Convention de Chicago, les règlements européens en matière d'aéronautique[368] ne s'appliquent pas aux aéronefs militaires et d'État mais prévoient également une obligation pour ces derniers de respecter les dispositions relatives aux règles générales de sécurité[369]. En d'autres termes, ils imposent l'application des règles de l'air à tout type d'aéronef par mesure de sécurité des autres aéronefs ainsi que des personnes et biens survolés. Concrètement, ces conventions internationales imposent aux États d'être en mesure de démontrer l'existence d'une exploitation des aéronefs militaires et d'État respectant des normes de sécurité et de garantir leur conformité aux normes techniques (état de l'appareil). Pour ce faire, la France a pris le parti d'adopter des règles similaires à celles de l'aéronautique civile au travers de textes réglementaires. En outre, ces règles sont applicables indifféremment aux aéronefs militaires et aux aéronefs d'État, la France ayant fait le choix de regrouper sous cette terminologie tout aéronef appartenant aux services de l'État et intervenant dans le cadre de fonctions régaliennes[370].

---

366 *Idem*, art. 3 (d).

367 *Idem*, art. 12.

368 Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil, *JOUE* du 22 août 2018, pp. 1-122 [en ligne] ; Règlement (UE) 923/2012 du 26 septembre 2012 établissant des règles de l'air communes et des dispositions opérationnelles relatives aux services et procédures de navigation aérienne, *JOUE* 13 octobre 2012 [en ligne].

369 Règlement (UE) 2018/1139 du 4 juillet 2018, art. 2 3) : « Les États membres s'engagent à faire en sorte que ces opérations ou activités soient menées en tenant dûment compte, dans la mesure du possible, des objectifs du présent règlement. Les États membres veillent également à ce que, le cas échéant, une séparation en toute sécurité soit établie entre ces aéronefs et les autres aéronefs ».

370 Décret n° 2013-366 du 29 avril 2013 portant création de la direction de la sécurité aéronautique d'Etat, *JORF* n°0102 du 2 mai 2013 [en ligne], art. 2 : « sont dénommés aéronefs d'État pour l'application du présent texte les aéronefs militaires ainsi que les aéronefs appartenant à l'État et utilisés par les services de douanes, de sécurité publique et de sécurité civile […] ».

150. Les drones dans le droit aérien international - La Convention de Chicago ne comporte qu'un seul article faisant référence aux aéronefs sans pilote à bord, qui constitue néanmoins une première règle capitale à l'encadrement des drones : « aucun aéronef pouvant voler sans pilote ne peut survoler sans pilote le territoire d'un État contractant, sauf autorisation spéciale dudit État et conformément aux conditions de [la convention]. Chaque État contractant s'engage à faire en sorte que le vol d'un tel aéronef sans pilote dans des régions ouvertes aux aéronefs civils soit soumis à un contrôle qui permette d'éviter tout danger pour les aéronefs civils »[371]. Cette règle s'adresse à tous les aéronefs sans pilote à bord sans tenir compte de leur caractère civil ou militaire et d'État. La Convention instaure trois conditions à l'introduction des drones dans l'espace aérien : un certificat de navigabilité, une certification de compétence des personnels en charge de l'aéronef et le respect des règles de l'air. Tout d'abord, elle introduit l'obligation pour tout aéronef d'obtenir un certificat de navigabilité[372] permettant d'attester des aptitudes au vol en sécurité d'un aéronef. Ensuite, le traité prévoit une obligation de qualification des pilotes[373]. Les pilotes de drones devront donc être formés et détenir des certificats d'aptitude. Enfin, la Convention met en place des règles de l'air[374] détaillées au sein de son Annexe 2[375]. Il revient aux États la responsabilité de faire respecter les règles de l'air aux aéronefs (civils comme militaires et d'État) qui survolent leur territoire.

151. Un encadrement hybride - L'évolution des aéronefs sans pilote à bord militaires et d'État au sein de l'espace aérien général nécessite, par conséquent, de respecter les règles concernant les aéronefs militaires et d'État auxquelles s'ajoutent celles liées à la sécurité du milieu dans lequel ils évoluent. Il n'existe pas de règlementation unifiée à l'usage des aéronefs sans pilote à bord militaires et d'État évoluant au sein de l'espace aérien général. Compte tenu de leur utilisation en milieu urbain, les drones de sécurité publique font donc l'objet d'une réglementation spécifique à caractère hybride empruntant des dispositions propres à l'aviation civile tout en reposant majoritairement sur des dispositions relatives à la règlementation nationale des aéronefs sans personne à bord militaires et d'État. Des dispositions tenant aux drones destinés à un usage

---

371 Convention de Chicago du 7 décembre 1944, *op. cit.*, art. 8.

372 *Idem*, art. 31 et Annexe 8 de la Convention relative à l'aviation civile internationale - Navigabilité des aéronefs, 1er mars 1949, OACI, 11e édition, juillet 2010, 212 p. [en ligne].

373 *Idem*, art. 32 (a) et Annexe 1 de la Convention relative à l'aviation civile internationale - Licence personnelle, 14 avril 1948, OACI, 11e édition, juillet 2011, 130 p. [en ligne].

374 *Idem*, art. 12.

375 Annexe 2 de la Convention relative à l'aviation civile internationale - Règles de l'air, mars 2012, OACI, 11e édition [en ligne].

civil peuvent ainsi leur être applicables afin d'assurer l'intégrité physique des personnes au sol ainsi que celle du drone. Dans un souci d'adaptation à l'environnement urbain dans lequel ils évolueront, l'introduction des drones de sécurité publique dans l'espace aérien national suppose le respect de deux régimes juridiques[376]: celui tenant aux textes relatifs aux aéronefs sans pilote à bord militaires et d'État utilisés à des fins de sécurité publique et civile (§1), d'une part, et celui dédié aux aéronefs sans pilote à bord utilisés au sein de l'espace aérien national (§2), d'autre part.

§1. Les dispositions réglementaires spécifiques à l'aéronautique d'État applicable aux drones de sécurité publique

152. Dans son rapport sur les drones des forces armées[377], en date du 23 mai 2017, le Sénat rappelait la nécessité pour les aéronefs sans pilote à bord militaires et d'État utilisés au sein de l'espace aérien général de se conformer aux règles de navigabilité. Il s'agit là d'une évidence, cette règle issue du droit aéronautique international s'appliquant à tout aéronef survolant le territoire d'un État. Comme tout aéronef, le drone est soumis à des règles tenant à sa conception, à ses conditions d'utilisation, à sa navigabilité, à son immatriculation ainsi qu'à son insertion au sein de l'espace aérien national. Le drone ne disposant pas d'un pilote à bord, les dispositions réglementaires se concentrent sur la préservation de l'intégrité physique des personnes survolées et des autres aéronefs. Plusieurs textes réglementaires ont été mis en œuvre en vue d'une utilisation d'aéronefs sans pilote à bord par des agents de la sécurité publique en milieu urbain (espace aérien général). Les drones de sécurité publique, en leur qualité d'aéronefs sans pilote à bord militaires et d'État, sont régis par les décrets du 29 avril 2013[378] et par l'arrêté du 24 décembre 2013[379].

153. Le décret du 29 avril 2013[380] définit les règles applicables en matière d'aéronefs militaires ou appartenant à l'État utilisés par les services de douanes, de sécurité publique ou civile,

---

376 HANICOTTE (R.), « Une nouvelle catégorie d'OVNI juridique : les drones », *op. cit.*

377 Sénat, Rapport d'information n° 559 (2016-2017) « Drones d'observation et drones armés : un enjeu de souveraineté » remis par PERRIN (C.) *et al.*, *op. cit.*

378 Décret n° 2013-367 du 29 avril 2013 relatif aux règles d'utilisation, de navigabilité et d'immatriculation des aéronefs militaires et des aéronefs appartenant à l'État et utilisés par les services de douanes, de sécurité publique et de sécurité civile, *JORF* n°0102 du 2 mai 2013 [en ligne] et Décret n° 2013-366 du 29 avril 2013 portant création de la direction de la sécurité aéronautique d'Etat, *op. cit.*

379 Arrêté du 24 décembre 2013 fixant les règles relatives à la conception et aux conditions d'utilisation des aéronefs militaires et des aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile qui circulent sans aucune personne à bord, *JORF* n°0302 du 29 décembre 2013 [en ligne].

380 Décret n° 2013-367 du 29 avril 2013, *op. cit*.

et soumet ces derniers à l'autorité de la Direction de la sécurité aéronautique d'État (DSAÉ). Il est intéressant de noter que le texte ne fait aucunement mention du terme « drone » et n'utilise que celui d'« aéronef ». Il n'existe pas à proprement parler de « drones » dans les textes de lois ou règlementaires, qui feront plutôt mention des termes d' « aéronefs sans pilote à bord » ou plus rarement d' « aéronefs télépilotés ». Le décret commence par spécifier son champ d'application, comprenant les aéronefs appartenant à l'État ainsi que les aéronefs n'appartenant pas à l'État mais utilisés dans le cadre de missions au service de l'État[381]. Il définit le terme « aéronef » comme « tous les appareils capables de s'élever ou de circuler dans les airs »[382]. En revanche, aucune des définitions ne précise si ces aéronefs comportent un pilote à bord ou si ceux-ci sont télépilotés. Il n'est fait mention des termes « d'aéronef sans pilote à bord » qu'à l'article 11 du décret et ce dans le cadre d'une dérogation à ce même décret. Il est, de fait, possible de déroger à ce décret sous réserve de respecter les dispositions particulières fixées par arrêté interministériel[383]. Le décret vient ensuite définir les différents documents et qualifications à obtenir en vue d'exploiter ce type d'aéronefs[384]. Le document de navigabilité peut être soit le certificat de navigabilité soit l'autorisation de vol. Le certificat de navigabilité est délivré par la DSAÉ. Le texte précise ensuite que l'aéronef ne peut être utilisé que par des pilotes qualifiés (disposant de l'autorisation et de l'immatriculation requises), évoluant selon les règles de navigabilité (document d'autorisation) et dans les conditions respectant le manuel d'utilisation du drone. Enfin, il définit le contenu du certificat de type[385] délivré par la Direction générale de l'aviation civile (DGAC), comprenant le type de produit, les pièces et équipements de celui-ci.

154. L'arrêté du 24 décembre 2013 concerne spécifiquement les aéronefs sans personne à bord. Il régit les aéronefs militaires et les aéronefs appartenant à l'État utilisés par les services de douanes, de sécurité publique et de sécurité civile évoluant uniquement sans personne à bord[386]. Ce texte complète le décret n° 2013-367 en n'y dérogeant que partiellement et non totalement, rendant

---

381 *Idem*, art. 1er.

382 *Idem*, art. 2.

383 En l'occurrence l'arrêté du 24 décembre 2013 décrit ci-après.

384 Décret n° 2013-367 du 29 avril 2013, *op. cit*., art. 4.

385 *Idem*, art. 5 et 7. Le certificat de type définit la famille à laquelle appartient un aéronef (ex. Mirage 2000, Rafale, etc.) et décrit sa composition.

386 Arrêté du 24 décembre 2013 fixant les règles relatives à la conception et aux conditions d'utilisation des aéronefs militaires et des aéronefs appartenant à l'Etat et utilisés par les services de douanes, de sécurité publique et de sécurité civile qui circulent sans aucune personne à bord, *op. cit.*, art. 1er.

le décret toujours applicable[387]. Là encore, le texte ne comporte aucune définition du terme « drone » et ne fait qu'un renvoi au décret n° 2013-637 qui mentionne « les aéronefs circulant sans personne à bord » en son article 11 ainsi qu'à quatre arrêtés du 3 mai 2013. L'arrêté du 24 décembre 2013 définit quant à lui les types d'aéronefs concernés selon leur mode de vol, leur masse et leur lieu d'exploitation (espace aérien ou espace clos). Il comprend cinq catégories d'aéronefs sans pilote à bord classés par catégories de masse et suivant qu'ils évoluent en espace clos ou en extérieur[388]. L'une de ces catégories concerne notamment les aéronefs dits « captifs » (M-0) qui, dans l'arrêté, comprennent les aéronefs « *rattachés au sol* » mais aussi ceux évoluant dans un « espace clos »[389] permettant notamment l'encadrement de petits drones utilisés afin d'explorer l'intérieur d'un bâtiment en proie aux flammes ou sinistré. Le texte définit également les conditions qualificatives d'un environnement dit « sensible » eu égard aux risques présentés pour les autres aéronefs de l'espace aérien général et du nombre élevé de la densité de population, qu'il s'agisse d'individus, d'animaux ou encore d'espaces tels que les zones industrielles. Cet arrêté régissant les aéronefs sans personne à bord militaires ou d'État utilisés à des fins de sécurité publique et de sécurité civile s'applique *de facto* aux drones à l'usage des forces de police, de la gendarmerie nationale et des sapeurs-pompiers.

155. Cette règlementation est apparue comme insuffisante aux yeux du Sénat, dans son rapport de 2017 précité, qui regrettait que les textes se contentent d'imposer le respect des conditions de navigabilité et ne permettent pas d'assurer le vol de ce type d'aéronefs en dehors d'espaces ségrégués. Un espace ségrégué peut être défini comme « une zone en trois dimensions […] attribuée [au drone], pour une durée déterminée, de laquelle il n'est pas censé sortir et dans laquelle aucun autre aéronef (*a fortiori* civil) n'est censé pénétrer »[390]. En d'autres termes, il s'agit de créer une forme de muraille virtuelle (ou *geofence*) afin d'empêcher un drone de sortir d'un espace délimité. Les drones de sécurité publique, par leur qualité d'aéronefs sans pilote à bord militaires et d'État, étaient donc limités à un vol en espace ségrégué lorsqu'ils évoluaient au sein de l'espace aérien général.

---

[387] POURCEL (E.), « Drone aérien : y-a-t-il un pilote « de » l'avion ? », *op. cit.*

[388] Arrêté du 24 décembre 2013, *op. cit.*, art. 3.

[389] *Idem*, art. 2. Le qualificatif d'« espace clos » fait référence à un aéronef sans pilote évoluant à l'intérieur d'un bâtiment.

[390] BROCAREL (A.), « L'insertion et la circulation des drones militaires dans les espaces nationaux », p. 92 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit*.

156. Néanmoins, la règlementation comprend des exceptions afin que ces aéronefs puissent évoluer au sein de l'espace aérien général dans certaines conditions. À cette fin, un décret du 20 avril 1995[391] prévoit des règles de compatibilité des engins aériens militaires avec l'espace aérien général permettant aux aéronefs militaires et d'État d'évoluer au sein de l'espace aérien général sous réserve de respecter la règlementation aérienne civile. Le décret soulignait toutefois l'importance de l'application du principe « voir et éviter » afin de prévenir tout risque de collision avec d'autres aéronefs. Cependant, les drones sont des aéronefs particuliers puisqu'ils sont contrôlés à distance (par conséquent sans pilote à leur bord), et ne peuvent par nature respecter le principe de « voir et éviter ». Il va de soi que le drone étant une machine il ne peut « voir » à proprement parler tel que le pourrait un être humain. Pourtant, il arrive que ces drones soient amenés à évoluer au sein d'un espace aérien non contrôlé (non ségrégué) et soient amenés à n'appliquer qu'un principe de « détecter et éviter ».

157. Afin de prévenir tout risque pour les autres usagers du ciel et pour les personnes survolées, un aéronef sans pilote à bord militaire et d'État utilisé à des fins de sécurité publique ou de sécurité civile dans l'espace aérien général doit respecter la règlementation relative aux aéronefs sans équipage à bord issue de l'aéronautique civile.

§2. Les dispositions réglementaires issues de l'aéronautique civile applicables aux drones de sécurité publique

158. Le premier cadre réglementaire assurant le vol des aéronefs civils sans pilote à bord a été adopté dès 2012[392] faisant de la France l'une des pionnières en matière d'encadrement juridique des aéronefs sans pilote à bord à usage civil[393]. Ces premiers arrêtés ont été révisés par ceux du 17

[391] Décret n°95-421 du 20 avril 1995 fixant les règles destinées à assurer la compatibilité des règles applicables à la circulation aérienne générale et à la circulation aérienne militaire, *JORF* n°95 du 22 avril 1995 [en ligne].

[392] Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent, *JORF* n°0109 du 10 mai 2012 et Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord, *JORF* n°0109 du 10 mai 2012.

[393] CHARLES (J-B.) et DUPONT (P.), « Fasc. 962 Drones civils - Notion, cadre et régime », *JCl. Transport*, 2 octobre 2018, màj le 31 mars 2021, p. 2.

décembre 2015[394] puis par ceux du 3 décembre 2020[395] (B). Ces révisions répondent à une nécessité tant de lisibilité que de clarté des dispositions régulant ces aéronefs et adaptent les dispositions nationales au cadre européen issu des règlements du 4 juillet 2018[396] et du 24 mai 2019[397] concernant l'exploitation d'aéronefs sans équipage à bord. Ces deux règlements sont venus compléter le *corpus* de textes relatifs à l'espace aérien européen (A).

A. L'influence du cadre européen sur la règlementation des drones aériens de sécurité publique

159. Depuis 1999, la Commission européenne s'applique à mettre en œuvre un projet d'unification des règles applicables à l'espace aérien européen et inaugure un plan intitulé « Ciel unique européen »[398]. Ce projet a finalement vu le jour en 2004 avec l'élaboration d'un corps de règlements instaurant le *Single European Sky Air traffic management Research*, destiné à favoriser le bon déroulement du processus de recherche et de développement de la gestion du trafic aérien. Ce *corpus* de règlements comprend ainsi des dispositions relatives aux règles de l'air ainsi que des dispositions encadrant l'exploitation d'aéronefs civils, dont les aéronefs sans pilote à bord.

160. Le règlement européen du 26 septembre 2012[399], dit « SERA » (*Standardised European Rules of the Air*), est venu définir les règles de l'air du territoire européen reprenant pour l'essentiel les diverses annexes issues de la Convention de Chicago du 7 décembre 1944[400] relative à l'aviation civile internationale (notamment son annexe 2). Ce Règlement prévoit des dispositions dérogatoires

---

394 Arrêté du 17 décembre 2015, dit « Conception », relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités des personnes qui les utilisent, *JORF* du 24 décembre 2015 [en ligne] et Arrêté du 17 décembre 2015, dit « Espace », relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord, *JORF* 24 décembre 2015 [en ligne].

395 Arrêté du 3 décembre 2020, dit « Espace », relatif à l'utilisation de l'espace aérien par les aéronefs sans équipage à bord, *JORF* n°0298 du 10 décembre 2020 [en ligne] et Arrêté du 3 décembre 2020, dit « Scénarios », relatif à la définition des scénarios standard nationaux et fixant les conditions applicables aux missions d'aéronefs civils sans équipage à bord exclues du champ d'application du règlement (UE) 2018/1139, *op. cit.*

396 Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, *op. cit.*

397 Règlement d'exécution (UE) 2019/947 de la Commission du 24 mai 2019 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord, *JOUE* L 152 du 11 juin 2019, pp. 45-71 [en ligne].

398 Communication de la Commission au Conseil et au Parlement européen, « La Création du ciel unique européen », COM(1999) 614 final, 1er décembre 1999, 39 p. [en ligne].

399 Règlement (UE) 923/2012 du 26 septembre 2012 établissant des règles de l'air communes et des dispositions opérationnelles relatives aux services et procédures de navigation aérienne, *op. cit.*

400 Convention de Chicago de 1944, *op. cit.*

concernant les activités d'intérêt public et notamment celles relatives aux missions policières et douanières, à la surveillance de la circulation et poursuites, à la recherche et au sauvetage, aux évacuations ou encore à la lutte contre les incendies[401].

161. Un premier règlement en date du 20 février 2008[402] est venu encadrer l'espace aérien européen. Ce texte comprenait des dispositions relatives aux aéronefs circulant sans équipage à bord avec cependant l'inconvénient de ne prendre en compte que les drones de plus de 150 Kg. En vue de pallier cette absence de cadre des drones de petites tailles, en plein essor, la Commission européenne, conjointement avec l'Agence Européenne de la Sécurité Aérienne[403] (AESA), a souhaité amender ce règlement. La Déclaration de Riga du 6 mars 2015[404] intitulée « *Définir l'avenir de l'aviation* » fut l'un des textes primordiaux ayant servi à l'élaboration de ce nouveau règlement européen permettant notamment l'encadrement des drones. À cette fin, le texte introduisait des propositions d'harmonisation du cadre règlementaire à l'usage des RPAS (« système d'aéronef télépiloté ») tenant compte du caractère primordial de la protection des droits et libertés des individus face à l'utilisation des drones. Ladite Déclaration met, en outre, l'accent sur la nécessité de protéger les droits des tiers sans pour autant enrayer l'innovation en introduisant plusieurs principes[405]. Ces propositions auront participé à l'adoption du nouveau règlement européen encadrant l'exploitation de l'espace aérien européen. Le Règlement européen relatif à l'aviation civile adopté le 4 juillet 2018[406] unifie ainsi le cadre relatif aux aéronefs, y compris ceux sans équipage à bord. Il met en œuvre des règles générales de sécurité à destination de tout type d'aéronef et comprend une section spécifique dédiée à l'usage des drones[407]. En outre, il permet une

---

401 Règlement (UE) 923/2012 du 26 septembre 2012, *op. cit.*, art. 4.

402 Règlement n°216/2008 du Parlement européen et du Conseil du 20 février 2008 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence européenne de la sécurité aérienne [en ligne] abrogé par le nouveau Règlement UE paru le 4 juillet 2018.

403 L'Agence Européenne de la Sécurité Aérienne (AESA) est l'organe de régulation et d'exécution des dispositions en matière de sécurité de l'aviation civile en Europe.

404 Riga Declaration on Remotely Piloted Aircraft (Drones) - 'Framing the Future of Aviation', Riga, 6 mars 2015 [en ligne]

405 Ces principes sont au nombre de cinq et comprennent : 1) Une intégration des drones dans l'espace aérien garantissant un niveau de sécurité proportionnel au risque encouru pour chaque opération ; 2) La mise en œuvre sans délai d'un cadre réglementaire européen pour les RPAS ; 3) Le développement de technologies clés manquantes et des normes requises ; 4) Le respect des droits fondamentaux des citoyens ; 5) La définition des conditions de responsabilité de l'exploitant d'un drone.

406 Règlement (UE) 2018/1139 du 4 juillet 2018, *op. cit.*

407 *Idem*, Section VII et Annexe IX relatifs aux « Aéronefs sans équipage à bord ».

évolution du cadre existant en supprimant la masse limite d'application de la règlementation en matière d'aviation civile.

B. Un cadre aéronautique civil adapté aux drones aériens de sécurité publique

162. L'entrée en vigueur, le 31 décembre 2020, du règlement européen de 2018 révisant le cadre de l'aéronautique civile a sensiblement modifié les dispositions du droit aérien français applicables aux drones évoluant au sein de l'espace aérien national. Les arrêtés de 2015, qui régissaient auparavant ces aéronefs, ont fait l'objet d'une révision par deux arrêtés d'application en date du 3 décembre 2020[408], dits « Espace » et « Scénarii », afin d'intégrer les nouvelles dispositions du règlement européen. Ces arrêtés opèrent d'importantes modifications du cadre relatif aux aéronefs sans pilote à bord. L'arrêt « Scénarii » refond les différents scénarii de vol propre à l'aéronautique civile en conservant, toutefois, les scénarii opérationnels de vol prévus dans les arrêtés précédents (à l'exception du scénario S4) jusqu'au 2 décembre 2023[409]. L'arrêté « Espace » remplace, quant à lui, les catégories d'activités (aéromodélisme, expérimentation et activités particulières) introduites par les précédents arrêtés par celles issues de la nouvelle règlementation européenne[410] (1). En dépit des améliorations substantielles que confère cette réglementation aux drones aériens de sécurité publique ceux-ci souffrent néanmoins d'un encadrement « dispersé » (2).

1. Les conditions de déploiement des drones aériens de sécurité publique

163. Conditions d'emploi - Le nouveau cadre juridique des drones évoluant au sein de l'espace aérien général intègre désormais trois catégories d'opérations qui reposent sur le niveau de risque présenté[411]. La catégorie « ouverte » s'adresse aux drones présentant des risques faibles tels

---

408 Arrêté du 3 décembre 2020, dit « Espace », relatif à l'utilisation de l'espace aérien par les aéronefs sans équipage à bord, *op. cit.* et Arrêté du 3 décembre 2020, dit « Scénarii », relatif à la définition des scénarios standard nationaux et fixant les conditions applicables aux missions d'aéronefs civils sans équipage à bord exclues du champ d'application du règlement (UE) 2018/1139, *op. cit.*

409 Règlement UE 2021/1166 du 15 juillet 2021 modifiant le règlement d'exécution (UE) 2019/947 en ce qui concerne le report de la date d'application des scénarios standards pour les exploitations effectuées en vue directe ou hors vue, art. 1er 4) *JOUE* L 253 du 16 juillet 2021, p. 49 [en ligne].

410 Celles-ci sont notamment détaillées dans le Guide de la DGAC, Guide « Usages des aéronefs sans équipage à bord : Catégorie spécifique », Édition 1, Version 1.7, *op. cit.*

411 Règlement d'exécution (UE) 2019/947 de la Commission du 24 mai 2019 concernant les règles et procédures applicables à l'exploitation d'aéronefs sans équipage à bord, *op. cit.*, art. 4, 5 et 6 ; Arrêté du 3 décembre 2020, dit « Espace », *op. cit.*, art. 2, 4°.

que des drones évoluant en vue du télépilote dans des endroits représentant un faible risque tant pour d'autres aéronefs que pour les personnes survolées. La catégorie « spécifique » intéresse les drones effectuant des opérations considérées comme présentant un risque modéré. Enfin, la catégorie « certifiée » est dédiée aux drones effectuant des opérations présentant des risques élevés. Les nouveaux arrêtés introduisent des dispositions permettant l'encadrement des aéronefs sans équipage à bord par les exploitants dont l'activité est exclue du champ d'application de la réglementation européenne. Ils peuvent par conséquent s'appliquer aux aéronefs sans personne à bord, militaires et d'État ou exerçant des missions pour le compte de l'État telles que des missions de police ou de secours. Dans le cadre de l'exploitation d'un aéronef sans pilote à bord, l'opération devra faire l'objet d'une autorisation spécifique délivrée par la Direction de la sécurité de l'aviation civile (DSAC)[412].

164. L'arrêté « Scénarii » prévoit que les aéronefs sans pilote à bord ne peuvent évoluer que dans le cadre des scénarii opérationnels qu'il définit ; à défaut, ils devront faire l'objet d'une demande d'autorisation spécifique délivrée par la DSAC. L'arrêté comprend trois types de scénarii de vol qui reposent sur différents critères, à savoir le mode de vol (en vue ou hors vue du télépilote), le lieu d'évolution (en zone peuplée ou non peuplée), la distance et la masse maximales de l'aéronef (charges utiles comprises[413]). Il dispose, en son annexe, d'un chapitre spécifiquement dédié à l'exploitation d'aéronefs sans équipage à bord à des fins de sauvegarde de l'ordre public et de sécurité civile explicitant les différentes obligations que sont tenus de respecter les exploitants. Lorsque la règlementation européenne entrera définitivement en vigueur, les aéronefs sans pilote à bord entrant dans la catégorie « spécifique » disposeront de deux scénarii de vol applicable à partir du 1er janvier 2024. Le premier scénario concerne les exploitations en vue directe et est très semblable au scénario national S3[414]. Le deuxième scénario s'applique aux exploitations hors de la vue du télépilote et s'assimile au scénario national S2[415].

---

412 *Idem*, pp. 12-13.

413 Les charges utiles sont toutes les éléments ou ensemble d'éléments que peut transporter l'aéronef. Il peut s'agir d'une caméra (afin de contrôler les déplacements de l'aéronef), d'une radio (permettant le contrôle de l'aéronef et la transmissions de données), d'une caméra de surveillance, d'un GPS (*Global Position System*/Système de Positionnement Global), ou encore d'un système LIDAR (*Light/Laser Detection and Ranging*) qui permet de détecter et d'estimer une distance par l'intermédiaire d'ondes lumineuses.

414 Guide de la DGAC, Guide « Usages des aéronefs sans équipage à bord : Catégorie spécifique », Édition 1, Version 1.7, *op. cit.*, p. 16.

415 *Ibid*.

165. L'arrêté « Espace », introduisant les nouvelles catégories d'exploitation de drones aériens, dispose que tout aéronef, hors catégorie « ouverte », évoluant en zone peuplée devra faire l'objet d'une déclaration préalable auprès du préfet territorialement compétent dans un préavis de cinq jours ouvrables[416]. Cependant, il relèverait de la gageure de vouloir effectuer une demande préalable d'exploitation d'un drone aérien lorsque celle-ci doit être effectuée en urgence particulièrement dans le cas des services de sécurité et de secours (ex. incendie ou attaque terroriste). Aussi, l'hypothèse de circonstances exprimant une urgence ou des circonstances imprévues[417] avait déjà été envisagée, tant par le décret 2013-367 du 29 avril 2013 que par les textes de 2015 (dont les dispositions sont reprises par les textes du 3 décembre 2020). À cette fin, un cadre dérogatoire est prévu par le décret de 2013[418] et les deux arrêtés[419] à destination des aéronefs sans pilote à bord militaires et d'État ou utilisés pour le compte de l'État. Un protocole dérogatoire à l'exploitation d'un aéronef sans pilote à bord dans le cadre d'une situation d'urgence a donc été mis en œuvre permettant au préfet territorialement compétent de valider le non-préavis de survol s'il estime que la situation le justifie. Il convient de noter que toute dérogation signée par le préfet ne constitue qu'une dérogation aux obligations administratives de survol. En d'autres termes, il existe une différence d'appréhension de la responsabilité entre les obligations administratives, d'une part, et le contrôle technique, d'autre part. Ces dispositions dérogatoires prévues pour les cas d'urgence et de nécessité absolue traduisent une véritable différence entre les règles applicables à l'aviation civile et celles relatives à l'aviation militaire et d'État.

166. Formation des télépilotes - Face aux risques que présentent l'utilisation de drones aériens dans l'espace urbain pour l'intégrité des personnes au sol, le droit aérien français a prévu des règles organisant la formation des télépilotes. Ces règles sont insérées dans plusieurs textes réglementaires relatifs à l'aéronautique militaire et à l'aéronautique civile. Les drones de sécurité

---

[416] Arrêté du 3 décembre 2020 dit « Espace », *op. cit.*, art. 6.

[417] À noter que les arrêtés de 2020 n'emploient cependant pas le terme d' « urgence » mais ceux de « circonstances qui le justifie ». La DGAC définit ces termes par « une situation d'urgence non programmable » ; en d'autres termes, tout évènement imprévisible qui peut faire l'objet d'une mission opérationnelle.

[418] L'article 10 du décret 2013-367 du 29 avril 2013 dispose que « en cas de circonstances exceptionnelles ou de nécessité opérationnelles urgentes, les autorités d'emploi mentionnées à l'article 3 du présent décret peuvent, par décision motivée et pour une durée limitée, déroger aux dispositions du présent décret ».

[419] L'article 9 de l'arrêté « Scénarii » dispose que « Les aéronefs sans équipage à bord utilisés dans le cadre de missions de recherche et de sauvetage, de lutte contre l'incendie, de douane, de police ou de sécurité civile ou activités analogues sous le contrôle et la responsabilité de l'État peuvent évoluer en dérogation aux dispositions du présent arrêté lorsque les circonstances de la mission le justifient ». De même, l'article 9 de l'arrêté « Espace » énonce que « Les aéronefs sans équipage à bord utilisés dans le cadre de missions de recherche et de sauvetage, de lutte contre l'incendie, de douane, de police ou de sécurité civile ou activités analogues sous le contrôle et la responsabilité de l'État peuvent évoluer en dérogation aux dispositions du présent arrêté lorsque les circonstances de la mission le justifient ».

publique entrent dans la catégorie des RPAS et sont par conséquent des drones télépilotés. À ce titre, la réglementation impose le suivi d'une formation préalable par les télépilotes pour tout vol de ce type d'aéronefs. Le décret du 29 avril 2013 dispose en ce sens qu' « un aéronef […] ne peut être utilisé que […] si les personnes assurant la conduite de l'aéronef ou des fonctions relatives à la sécurité à bord détiennent les qualifications requises »[420]. De même, l'arrêté du 3 décembre 2020 dit « Scénarii » comprend des dispositions relatives au niveau théorique et pratique des télépilotes dans ses annexes[421]. Enfin, le décret du 2 février 2018[422] et l'arrêté du 18 mai 2018[423] relatifs à la formation des télépilotes d'aéronefs sans pilote à bord viennent définir les conditions nécessaires au pilotage des aéronefs sans pilote à bord hors catégorie « ouvert ».

167. Les autorités publiques exploitant des aéronefs sans pilote à bord ont un devoir de s'assurer de la formation de leurs agents (les télépilotes). À cette fin, l'arrêté prévoit les conditions d'examen des télépilotes nécessaires à l'obtention du certificat d'aptitude théorique de télépilote, de la formation pratique basique, de l'examen pratique en vue de l'obtention de la licence de télépilote et des conditions relatives à cette licence. Chaque télépilote devra obtenir un certificat d'aptitude théorique[424] (délivré par le ministre de l'Aviation civile) ainsi qu'une attestation de suivi de formation[425] (délivrée par l'exploitant chargé de la formation).

2. Un cadre réglementaire éclaté des drones aériens de sécurité publique

168. L'évolution de la réglementation française applicable aux aéronefs sans pilote à bord utilisés en milieu urbain démontre la volonté des autorités publiques d'assurer des conditions de vol sécurisées. L'objectif premier du recours à ces aéronefs était de faciliter l'exercice des missions des agents des forces de l'ordre et des services de secours en respectant les règles établies en matière de sécurité aérienne. En cela, les rédacteurs de cette réglementation sont parvenus à mettre en œuvre

---

[420] Décret n° 2013-367 du 29 avril 2013, *op. cit.*, art. 4, 5°.

[421] Selon l'article L. 6511-1 du Code des transports, le télépilote doit être en possession d'une attestation de compétence ainsi que « de titres aéronautiques et de qualifications dans des conditions déterminées par voie réglementaire ».

[422] Décret n°2018-67 du 2 février 2018 relatif à la formation exigée des télépilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir, *JORF* n°0029 du 4 février 2018 [en ligne] modifié par le décret n° 2019-660 du 26 juin 2019, *JORF* n°0148 du 28 juin 2019 [en ligne].

[423] Arrêté du 18 mai 2018 relatif aux exigences applicables aux télépilotes qui utilisent des aéronefs civils circulant sans personne à bord à des fins autres que le loisir, *JORF* n° 0129 du 7 juin 2018 [en ligne].

[424] CAC, art. D.136-2.

[425] CAC, art. D.132-2.

des garanties légales et techniques visant à prévenir les atteintes portées à l'intégrité physique des personnes au sol et les entraves causées à d'autres aéronefs évoluant au sein de l'espace aérien national.

169. La réglementation nationale relative aux drones aériens n'a pas été créée de toute pièce et repose sur une longue contribution jurisprudentielle en matière de responsabilité administrative ainsi que sur la règlementation aérienne en constante adaptation aux particularités de chaque type d'aéronef[426]. L'arrêt *Blanco* du 8 février 1873[427], en initiant le droit de la responsabilité administrative, a permis à l'État de qualifier sa responsabilité en fonction de ses impératifs faisant ainsi bénéficier ses agents d'une protection dans le cadre de l'exercice de leurs missions (exception faite d'une faute personnelle de ces derniers[428]). Cette jurisprudence administrative permet aux agents de ne pas être tenus personnellement pour responsable des actions effectuées dans le cadre de leurs fonctions qui auraient engendré un dommage et en engageant la responsabilité administrative des services de l'État (v. **n° 696 et suiv.**). Par conséquent, cette décision pourrait s'avérer particulièrement adaptée au cadre d'utilisation des drones aériens en milieu urbain dans la mesure où des dommages pourraient advenir aux personnes observées, principalement du fait d'une chute, sans pour autant résulter d'une faute personnelle de l'agent telle qu'une négligence ou un usage illégal. Or, cette réglementation aérienne constitue le premier pas permettant à ces aéronefs sans pilote à bord de participer aux actions des forces de l'ordre et des services de secours visant notamment à la sécurité des personnes et des biens, qui s'inscrit dans les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions.

170. Néanmoins, cette réglementation pourrait être encore améliorée. Il est à déplorer que le cadre juridique des drones aériens souffre d'une disparité dans ses sources, entrainant une complexification de son appréhension par les différents acteurs tant dans sa lisibilité que dans son accessibilité[429]. La réglementation applicable aux drones de sécurité publique s'avère tout

---

426 BROCAREL (A.), « L'insertion et la circulation des drones militaires dans les espaces nationaux », p. 95 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit*.

427 TC, 8 février 1873, Décision n° 00012, *Blanco* [en ligne].

428 TC, 30 juillet 1873, Décision n° 00035, *Pelletier* [en ligne] : Cette décision a permis d'introduire la distinction entre faute personnelle et faute de service (la deuxième permettant d'exonérer l'agent de sa responsabilité personnelle).

429 GOJKOVIC-LETTE (J.) et HOUILLON (G.), « La pratique du drone, entre sécurisation et répression », *AJP* n°3, 26 mars 2019 p. 135.

particulièrement complexe au regard de la disparité de ses sources au sein du droit européen et du droit national[430], d'une part, ainsi que des disciplines du droit[431], d'autre part. Comme d'autres outils numériques, les drones aériens associent différentes branches du droit ne permettant pas une unification de leur cadre juridique et une facilitation de sa lisibilité.

171. La réglementation européenne en matière de drones aériens a permis d'améliorer leur encadrement tant juridique que technique (en instaurant une classification de ceux-ci non plus en fonction de leur masse et de leur finalité d'emploi mais au regard du niveau de risque qu'ils présentent). Cependant, elle vient également se superposer au cadre juridique national toujours en vigueur qui s'applique en matière de drones aériens de sécurité publique. De fait, les aspects relatifs à la sécurité publique relèvent de la compétence nationale et s'additionnent aux dispositions issues du cadre européen, notamment s'agissant des mesures de sûreté publique[432] tout comme celles relevant de la collecte des données personnelles dans le cadre pénal[433]. En outre, la réglementation applicable aux drones aériens de sécurité publique est vouée à évoluer puisque la réglementation européenne est d'application progressive. En ce sens, l'arrêté « Scénarios » du 3 décembre 2020[434], comprenant des dispositions applicables aux exploitants de drones aériens qui n'entrent pas dans le champ de la réglementation européenne, telles que les missions de police, de secours ou encore de lutte contre les incendies, ne sera plus en vigueur à partir du 2 décembre 2023[435].

172. Enfin, ces aéronefs à l'usage des forces de l'ordre et des services de secours ne démontrent véritablement d'utilité que dans la mesure où ils évoluent en support d'autres technologies telles que des caméras et autres capteurs de données[436]. En outre, leur efficacité repose

---

[430] Elle associe des dispositions relevant du droit européen à des dispositions réglementaires issues du droit national.

[431] De manière non-exhaustive, les différentes dispositions sont intégrées au sein du CSI, du code des transports, du code civil (ex. droit à l'image, droit à la vie privée, etc.), du code pénal, ou encore du code de la protection des données personnelles.

[432] ARCHAMBAULT (L.) et ROTILLY (C.), « Vers une nouvelle réglementation européenne des drones », *Dalloz IP/IT* n° 3, 22 mars 2021, p. 163.

[433] La Directive européenne en matière de protection des données dans le cadre pénal (DPJ) n'est pas d'application directe puisqu'elle aborde des aspects qui relèvent de la souveraineté des États.

[434] Arrêté du 3 décembre 2020, dit « Scénarii », relatif à la définition des scénarios standard nationaux et fixant les conditions applicables aux missions d'aéronefs civils sans équipage à bord exclues du champ d'application du règlement (UE) 2018/1139, *op. cit.*

[435] ARCHAMBAULT (L.) et ROTILLY (C.), « Vers une nouvelle réglementation européenne des drones », *op. cit.*

[436] CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, pp. 98-99.

sur l'association de leur emploi à celui d'algorithmes en charge du traitement des données collectées pouvant potentiellement inclure une analyse en temps réel. Ce n'est alors qu'à la condition qu'il soit en mesure de collecter des données qu'un drone aérien pourra être caractérisé comme étant de « sécurité publique » et entrer dans le cadre des systèmes de vidéoprotection. Aussi, cette réglementation aérienne, bien que nécessaire, ne constitue véritablement qu'une étape « technique » du recours aux drones en milieu urbain par les forces de sécurité publique. En d'autres termes, cette réglementation ne suffit pas à régir l'usage de drones aériens équipés de caméras et autres capteurs de données. Pourtant, les forces de l'ordre n'ont pas hésité à faire usage de cette technologie dès qu'elles en ont eu l'occasion, sans prendre suffisamment en considération les conséquences qu'engendrait la collecte de données par ces aéronefs équipés de caméras sur les droits et libertés. L'existence de cette réglementation aérienne à l'usage des drones leur a visiblement laissé l'impression que les seuls verrous juridiques étaient liés à leur évolution en milieu urbain.

173. Conclusion - Les lois en matière de vidéoprotection s'inscrivent indubitablement dans cette tendance générale du législateur de se contenter de faire entrer dans la législation des pratiques depuis longtemps à l'œuvre et de concéder des prérogatives toujours plus importantes aux autorités publiques. L'association de caméras surveillant la voie publique aux technologies algorithmiques n'y fait pas exception compte tenu de l'insuffisance d'encadrement juridique entourant l'usage des algorithmes[437], particulièrement en matière de sécurité publique. Ce mouvement visant à renforcer la prévention des infractions plus que leur simple répression participe de ce privilège accordé à la sécurité au détriment de la sûreté. Pourtant, c'est bien la sûreté qui assure à elle seule cette conciliation entre la protection de l'État et la sauvegarde de l'ordre public, d'une part, et la protection des droits et des libertés de chacun, d'autre part.

[437] Voir notamment en ce sens : Sénat, Rapport d'information n° 464 (2016-2017) « Pour une intelligence artificielle maîtrisée, utile et démystifiée » remis par DE GANAY (C.) et GILLOT (D.), 15 mars 2017, p. 149 [en ligne] ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*

CHAPITRE 2 L'ENCADREMENT JURIDIQUE PERFECTIBLE DES CAMÉRAS AÉROPORTÉES « AUGMENTÉES » DE SÉCURITÉ PUBLIQUE

174. Face aux nouvelles technologies, le droit doit continuellement s'adapter. Les drones aériens de sécurité publique n'ont pas fait exception à la règle et ont nécessité l'élaboration d'un cadre spécifique à l'usage de ces nouveaux outils de vidéoprotection. Toutefois, leur introduction dans la législation ne s'est pas faite sans heurt. Le cadre juridique visant à autoriser l'utilisation des drones aériens par les forces de l'ordre et les services de secours a rencontré de nombreuses difficultés avant de voir le jour. L'élaboration d'un cadre juridique adapté a fait face à une importante controverse de la part des différents défenseurs des droits et libertés (d'origine institutionnelle, universitaire ou associative)[438]. Néanmoins, l'introduction de dispositions visant à encadrer le recours à des drones aériens de sécurité publique s'est avéré nécessaire compte tenu des usages qui en étaient déjà fait par les forces de l'ordre et les services de secours en l'absence de tout cadre spécifique à leur emploi (**Section 1**).

175. Les progrès techniques qu'apportent les drones aériens de sécurité publique ne reposent pas seulement sur leur capacité à collecter des données. En vue de maximiser leur efficacité lors des missions, les agents des forces de l'ordre et des services de secours souhaitent avoir recours à des algorithmes destinés à analyser les données collectées. Les technologies associant des algorithmes aux caméras de surveillance sont de plus en plus présentes et suscitent grandement l'intérêt des forces de l'ordre. Certains usages ont déjà pu être observés en Chine ou aux États-Unis mais aussi en Europe. Pourtant, l'emploi de dispositifs vidéo dits « intelligents » pouvant potentiellement inclure des algorithmes dits « prédictifs » ne fait encore l'objet d'aucun encadrement adapté. Or, l'utilisation de ces technologies, plus particulièrement dans un cadre régalien, soulève

---

[438] Pour la Commission nationale consultative des droits de l'homme (CNCDH), « Avis sur la proposition de loi relative à la sécurité globale » (A - 2020 - 16), 26 novembre 2020, *JORF* n°0289 du 29 novembre 2020 [en ligne]. Pour la CNIL, Délibération SAN-2021-003 du 12 janvier 2021 concernant x [en ligne] ; Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, avis n° 20020769 [en ligne] ; « Audition devant la Commission des lois du Sénat dans le cadre de l'examen de la proposition de loi relative à la sécurité globale », 3 février 2021 [en ligne] ; Délibération n°2021-078 du 8 juillet 2021 portant avis sur un projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, *op. cit.*. Pour le Défenseur des droits (DDD), avis n°20-05 du 3 novembre 2020 relatif à la proposition de loi sur la sécurité globale, p. 3 [en ligne] ; avis n°20-06 du 17 novembre 2020 relatif au texte adopté par la commission des lois, sur la proposition de loi relative à la sécurité globale, pp. 4-5 [en ligne] ; avis n°20-13 du 21 décembre 2020 relatif à la proposition de loi relative à la sécurité globale, pp. 3-4 [en ligne] ; avis n°21-12 du 20 septembre 2021 relatif au projet de loi sur la responsabilité pénale et la sécurité intérieure, pp. 6-9 [en ligne]. Voir également : Syndicat de la magistrature, « Observations du Syndicat de la magistrature sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure - Volet n°3 : dispositions relatives à la surveillance (Articles 7, 8, 9) », *op. cit.* ou encore les nombreux articles publiés à ce sujet par la Quadrature du Net [en ligne].

d'importantes problématiques pour les droits et libertés (**Section 2**).

Section 1 L'introduction législative controversée des drones aériens de sécurité publique

176. Ces vingt dernières années, les drones aériens de sécurité publique ont pleinement pris place au sein des outils à l'usage des forces de l'ordre et des services de secours et se sont progressivement imposés comme un outil prometteur à l'exercice de leurs fonctions. Néanmoins, ces caméras aéroportées de surveillance de la voie publique, à l'instar des caméras individuelles, ont longtemps souffert de l'absence d'un cadre juridique adapté (§1). La validation partielle par le Conseil constitutionnel des dispositions de la loi RPSI[439] du 24 janvier 2022 proposant un encadrement de l'usage de ces caméras par les forces de l'ordre (police et gendarmerie nationales) et les services de secours, a permis d'introduire dans le CSI et dans le CPP un régime juridique qui leur est propre non sans conserver certaines faiblesses (§2).

§1. Un encadrement juridique à l'usage des drones aériens de sécurité publique : un exercice périlleux

177. Avant la loi du 24 janvier 2022, les drones aériens de sécurité publique étaient soumis - par défaut - au cadre juridique existant en matière de police administrative ou de police judiciaire[440]. Leur encadrement se limitait aux normes règlementaires régissant leur emploi[441] et aux dispositions générales relatives à la vidéoprotection. En outre, ils pouvaient être soumis à la règlementation relative à la protection des données qui leur était applicable lorsque leurs enregistrements comportaient « des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques »[442] (A). Ce cadre s'est rapidement révélé être inadapté aux particularités des drones aériens, compte tenu des nouveaux enjeux en termes d'incidences sur la vie privée tenant aux avancées technologiques ainsi qu'à la mobilité dont ils bénéficient. Ces qualités font que les drones de sécurité publique présentent

---

[439] Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure (RPSI), *op. cit.*

[440] Sénat, Rapport n°46 (2021-2022) sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, remis par JOURDA (M.) et HERVÉ (L.), 13 octobre 2021, p. 56 s. [en ligne].

[441] Voir la Section 2 du Chapitre précédent sur la réglementation aérienne.

[442] CSI, art. L. 252-1.

un caractère disruptif qui réside tant dans leurs capacités à survoler les évènements qu'à observer et collecter un grand nombre et une diversité de données. Aussi, compte tenu des risques que présentent les drones aériens collectant des données, la CNIL suit depuis plusieurs années avec la plus haute attention les évolutions concernant leur développement et leur incidence sur la vie privée des personnes filmées. En 2013, elle publia, en ce sens, un article faisant part de ses inquiétudes au regard d'une possible « captation de masse sans distinction susceptible d'être opérée par les drones »[443]. Une première loi avait alors tenté d'offrir un encadrement juridique adapté à l'usage spécifique des drones aériens dans un cadre de sécurité publique (B).

A. Le cadre juridique des drones aériens de sécurité publique avant la loi RPSI

178. L'existence d'une législation stricte et protectrice des droits et libertés permettant l'encadrement du recours aux drones aériens à des fins de police administrative comme de police judiciaire a longtemps fait défaut. Dans son avis sur les usages de caméras aéroportées, le Sénat relevait qu'en dépit de leurs qualités, les drones aériens ne bénéficiaient pas d'un encadrement juridique autorisant explicitement leur usage par les forces de l'ordre et les services de secours[444]. En ce sens, il constatait que seul l'usage des drones civils avait fait l'objet d'un encadrement législatif spécifique. Dès lors, seules quelques rares dispositions pouvaient s'appliquer aux cas d'une captation d'images par ce type d'aéronef (1). Pour autant, le défaut de législation adaptée à l'usage de drones aériens de sécurité publique n'a en rien fait obstacle au recours par les forces de l'ordre, notamment lors de la crise sanitaire en 2020 (2).

1. L'absence d'encadrement adapté à l'usage des drones aériens de sécurité publique

179. Avant de disposer de leur propre régime juridique, les drones aériens de sécurité publique n'étaient encadrés que par quelques rares dispositions tenant à la captation d'images. La législation française permettait, dans certains cas, la captation d'images par un drone sous réserve de respecter

443 CNIL, « Drones, innovations, vie privée et libertés individuelles », *La lettre Innovation et Prospective*, n°6, décembre 2013 [en ligne].

444 CE, Avis n°401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, *op. cit.*, p. 1

l'article D133-10 du CAC[445] ainsi que son arrêté d'application du 27 juillet 2005[446]. Néanmoins, cette disposition n'offre en réalité qu'une faible garantie des droits et libertés compte tenu du fait qu'elle ne prend pas en compte la « miniaturisation » des drones, qui les rend difficile à détecter. En outre, celle-ci n'interdit pas le survol de propriétés privées par un aéronef[447].

180. Hormis ces dispositions, les drones aériens n'étaient soumis qu'au régime général de la vidéoprotection inscrit dans le CSI. Cependant, cet encadrement « de fortune » présentait de nombreuses limites liées à une mise en œuvre dédiée aux seules caméras fixes, qui ne prenait pas en compte les particularités propres au caractère mobile des drones aériens. Ce cadre comprenait néanmoins quelques dispositions pouvant s'appliquer aux drones de sécurité publique permettant les prises de vue de la voie publique[448] incluant la transmission et l'enregistrement de fichiers vidéo sous le contrôle des autorités publiques compétentes[449]. Ainsi, certaines des finalités énoncées à l'article L. 251-2 du CSI pouvaient convenir à l'utilisation des drones aériens sous réserve que leur intervention se limite à des évènements ponctuels nécessitant ce type d'outil de surveillance mobile comme il en est pour les caméras fixes. En ce sens, les finalités exceptionnelles prévues lors de situations d'urgence[450] semblaient davantage convenir à l'usage des drones aériens tel que le déclenchement d'un incendie ou le signalement d'un évènement mettant en péril la vie d'une ou de plusieurs personnes (ex. personne(s) armées menaçant la vie d'autrui). Aussi, la finalité tenant à « la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens »[451] pouvaient également se justifier - sous réserve d'un examen minutieux de proportionnalité. Ces finalités s'avéraient déjà

---

445 CAC, art. D 133-10, al. 6 :« Toute personne qui souhaite réaliser des enregistrements d'images ou de données dans le champ du spectre visible au-dessus du territoire national est tenue de souscrire une déclaration au plus tard quinze jours avant la date ou le début de période prévue pour l'opération envisagée auprès du chef du service territorial de l'aviation civile dont relève son domicile ».

446 Arrêté du 27 juillet 2005 portant application de l'article D. 133-10 du Code de l'aviation civile, *JORF* n°175 du 29 juillet 2005 [en ligne].

447 Code des transports, art. L. 6211-3. Il convient de préciser que « lorsqu'un bien (maison, jardin, etc.) est représenté, l'autorisation de son propriétaire, n'est en principe pas requise [sauf dans le cas où le bien constitue une œuvre architecturale qui nécessitera l'autorisation de son auteur car celle-ci est soumise aux droits d'auteur]. Toutefois, le propriétaire peut reprocher à l'utilisateur d'une photographie de son bien une exploitation qui lui causerait un trouble anormal (par exemple une publication de l'image de sa maison qui porterait atteinte à sa vie privée) » [en ligne].

448 BOURGEOIS (M.) et TOUZANNE (B.), « Les aéronefs civils télépilotés avec capteurs : des 'drones de droit' », *Communication - Commerce électronique* n°12, décembre 2015, étude 22.

449 CSI, art. L. 223-1.

450 CSI, art. L. 223-4 et L. 223-5.

451 CSI, art. L. 252-6 et L. 252-7.

particulièrement adaptées au cas des drones aériens en offrant l'opportunité aux agents de sécurité publique de réagir rapidement en vue de préserver l'ordre public[452]. Néanmoins, la limitation de leur recours à des finalités bien spécifiques et encadrées n'était pas prévue par le CSI. Plusieurs des finalités et garanties issues du cadre général de la vidéoprotection ont, par la suite, été reprises lors de l'élaboration du cadre afférent aux drones de sécurité publique. Ce fut le cas lors des deux propositions de texte visant à légiférer sur l'utilisation de ces drones dans le cadre de la surveillance de la voie publique avec, toutefois, d'importantes lacunes dans les moyens suggérés afin de mettre en œuvre ces garanties.

181. Afin de respecter les droits et libertés des personnes filmées, le cadre général de la vidéoprotection comprend plusieurs obligations qui peuvent également s'appliquer aux drones aériens de sécurité publique. Les utilisateurs de dispositifs de vidéoprotection sont tenus de respecter un devoir d'information du public[453]. Ils ont également pour obligation de limiter le périmètre des lieux pouvant être filmés afin de ne filmer que les espaces publics[454]. Aussi, les enregistrements effectués par ces caméras ne peuvent être conservés que pour une durée limitée au-delà de laquelle ceux-ci doivent être détruits[455] (hormis le cas où les événements donneraient lieu à l'ouverture d'une procédure judiciaire ou administrative). Enfin, dans un souci de préserver la confidentialité des données collectées, l'accès aux enregistrements doit être limité aux seules personnes habilitées[456]. Par ailleurs, le recours par les forces de l'ordre à des caméras filmant la voie publique engendre d'autres obligations issues du cadre relatif à la protection des DACP. Les autorités publiques sont ainsi tenues d'effectuer une analyse d'impact sur la protection des DACP permettant d'évaluer les risques potentiels (tant du point de vue informatique que juridique) des traitements effectués par des drones aériens filmant la voie publique[457]. Aussi, elles sont tenues de consulter l'autorité de contrôle nationale de protection des données (CNIL) qui analysera au préalable le traitement envisagé[458]. C'est précisément sur ce point de la règlementation que les

---

[452] LATOUR (X.), « La vidéoprotection et les collectivités territoriales » *in* DANTONEL-COR (N.) (dir.), *Les politiques publiques locales de sécurité intérieure*, *op. cit.*, p. 277.

[453] CSI, art. L. 251-3.

[454] *Idem*.

[455] CSI, art. L. 252-5.

[456] CSI, art. L. 252-2.

[457] LIL, art. 90 et DPJ, art. 27.

[458] LIL, art. 90 DPJ, art. 28.

forces de l'ordre ont failli à leurs obligations lorsqu'elles ont eu recours à des drones aériens afin de faire respecter les règles sanitaires durant l'état d'urgence en 2020[459].

2. Le besoin d'encadrement des drones aériens à l'usage des forces de l'ordre

182. Les autorités publiques n'ont pas hésité à avoir recours à des drones aériens alors qu'aucune législation propre à leur usage à des fins de police judiciaire ou de police administrative n'avait été adoptée[460]. La professeure Marthe Bouchet admet que dans le cadre de la procédure pénale « l'application du principe de légalité, qui oblige la loi pénale à prévenir avant de frapper[461] est discutée[462], mais [rappelle que] l'usage d'un nouveau moyen d'enquête doit être autorisé par un texte »[463]. Les révélations médiatiques[464] du recours à des drones de sécurité publique par les forces de l'ordre lors des confinements de 2020, sous le prétexte de l'état d'urgence sanitaire, a cependant réveillé les consciences. Les drones de sécurité publique ont nettement profité des confinements liés à la pandémie afin de s'imposer comme le nouvel outil de surveillance et de préservation de l'ordre public par les forces de l'ordre. L'usage de ces drones aériens filmant la voie publique a soulevé l'inquiétude des défenseurs des droits et libertés, qui y ont vu des outils de collecte massive de données à caractère personnel sans encadrement juridique strict.

183. Le recours à des drones de surveillance par la Préfecture de police de Paris durant la crise du coronavirus de 2020 a suscité de vives réactions et relancé le débat entourant leur emploi au point de mener deux associations de défense des droits, *La Quadrature du Net* et la *Ligue des droits de l'Homme*, à déposer un référé liberté afin de faire cesser immédiatement toute utilisation de drones à des fins de contrôle du respect des mesures de confinement. Dans un premier temps, les deux associations furent déboutées par le Tribunal administratif de Paris qui, dans sa décision du 5

---

459 LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *op. cit.*

460 *Idem* ; CNIL, « Suspension de l'utilisation des drones pour contrôler le déconfinement à Paris par le Conseil d'État : les contrôles de la CNIL », 18 mai 2020 [en ligne] ; LE FOLL (C.) et POURÉ (C.), « Profitant du flou juridique, les drones policiers bourdonnent toujours », *Médiapart*, 26 octobre 2020 [en ligne] consulté le 30 octobre 2020.

461 DDHC, art. 7 et Conv.EDH, art. 7.

462 Elle cite en ce sens LASSALLE (M.), « À la recherche du principe de légalité procédurale en matière pénale », *Rec. Dalloz*, 2020, p. 1196.

463 BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *op. cit.*

464 Voir principalement : LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *op. cit.*

mai 2020[465], avait rejeté leur demande au motif qu'il n'était pas établi ou soutenu que les drones auraient été utilisés à des fins d'identification des individus au sol. À l'appui de cette décision, la Préfecture de police de Paris avait notamment affirmé que les prises de vue ne permettaient pas l'identification des individus.

184. Par la suite, les deux associations avaient interjeté appel de cette décision devant le Conseil d'État qui s'est prononcé en leur faveur. Dans sa décision du 18 mai 2020[466], le Conseil d'État avait d'abord reconnu une finalité légitime à l'utilisation de drones dans le cadre de l'état d'urgence sanitaire et avait admis, par conséquent, que l'utilisation de drones en elle-même n'était pas de nature à porter une atteinte grave et manifestement illégale aux libertés fondamentales. Néanmoins, il soulignait que le dispositif litigieux effectuait un traitement de DACP qui relève *de facto* du champ d'application de la DPJ, nécessitant l'obtention d'une autorisation par décret ou arrêté après avis motivé de la CNIL. En l'espèce, le Conseil d'État avait estimé qu'au regard des risques pour la protection des DACP que présentait le recours à des drones aériens pour le compte de l'État effectuant un traitement de DACP sans autorisation par un texte règlementaire constituait « une atteinte grave et manifestement illégale au droit au respect de la vie privée »[467]. Ainsi, les juges avaient condamné l'exercice de la surveillance par drone aérien sur le fondement de la licéité et non de la proportionnalité eu égard au contexte exceptionnel d'état d'urgence sanitaire.

185. En conséquence, le Conseil d'État avait « enjoint l'État de cesser, sans délai, de procéder aux mesures de surveillance par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement »[468]. Cette décision fut immédiatement saluée par la CNIL qui avait approuvé la décision rendue par le Conseil d'État. Elle estimait, en ce sens, que ces drones, équipés de caméras ayant la possibilité de zoomer et d'identifier des personnes physiques, devaient à cette fin être soumis à la règlementation relative à la protection des DACP et qu'ils évoluaient donc hors du cadre de la LIL[469]. En outre, elle avait tenu à rassurer le public précisant que des procédures de contrôle de ces dispositifs étaient en cours. La décision du Conseil d'État fut

---

[465] TA Paris, ord., 5 mai 2020, n°2006861/9 [en ligne].

[466] CE, ord., 18 mai 2020, n°440442 [en ligne].

[467] *Idem*, cons. 18.

[468] *Idem*, cons. 19.

[469] CNIL, « Suspension de l'utilisation des drones pour contrôler le déconfinement à Paris par le Conseil d'État : les contrôles de la CNIL », *op. cit.*

alors perçue comme une victoire par les défenseurs des droits avant de rapidement laisser place à une certaine désillusion lorsque la Préfecture de police de Paris eut de nouveau recours à des drones aériens à des fins de surveillance lors du second confinement.

186. De fait, dans le courant des mois de novembre-décembre 2020, les drones furent de nouveau utilisés par les forces de l'ordre de la Préfecture de police de Paris ravivant dans leur sillage la polémique autour de ce mode de surveillance[470] et entrainant une seconde saisine du Conseil d'État. Dans sa décision rendue le 22 décembre 2020[471], il a confirmé sa position d'interdire aux forces de l'ordre de Paris l'emploi de drones pour surveiller les manifestations tant qu'un cadre législatif adapté n'aura pas été adopté. Ces événements se sont déroulés alors que le Parlement était encore en plein débat sur le projet de loi pour une sécurité globale qui entendait notamment adopter des dispositions visant à encadrer les drones aériens de sécurité publique. Lors des discussions, de nombreux sénateurs et députés s'étaient opposés à ces dispositions, estimant qu'elles étaient attentatoires aux libertés individuelles. À l'inverse du législateur, le Conseil d'État s'était montré plus rigoureux face à l'utilisation des drones aériens par les forces de l'ordre lors de sa seconde décision. En outre, il avait invité le Gouvernement « à réexaminer les différents régimes existants de captation d'images auxquels ont recours les autorités publiques, dans le cadre de leur mission de police administrative ou judiciaire », plus particulièrement au regard des dispositions relatives à la protection des DACP[472].

187. Ces multiples recours à des drones aériens équipés de caméras par les forces de l'ordre a également fait l'objet d'une décision de la CNIL. Celle-ci a ainsi prononcé un rappel à l'ordre à l'encontre du ministre de l'Intérieur pour avoir procédé, en dehors de tout cadre légal, à des vols de drones équipés de caméras, notamment en vue d'assurer le respect des mesures de confinement[473]. Dans sa décision, la CNIL a rappelé que « la captation, la transmission, la modification ou la consultation – portant sur l'image de personnes pouvant être reconnues constitue un traitement de

---

[470] LE FOLL (C.) et POURÉ (C.), « Profitant du flou juridique, les drones policiers bourdonnent toujours », *op. cit.* ; « Drones en manifestation : La Quadrature contre-attaque », *La Quadrature du Net*, 26 octobre 2020 [en ligne] consulté le 30 octobre 2020.

[471] CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155 [en ligne].

[472] CE, Avis consultatif n° 401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, 20 septembre 2020, *op. cit.*, p. 5.

[473] CNIL, Délibération n°SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'Intérieur, *op. cit.* Il convient de préciser que cette décision a, depuis, été anonymisée : « Délibération de la formation restreinte n°SAN-2021-003 du 12 janvier 2021 concernant x » [en ligne].

données à caractère personnel »[474] et que de ce fait « l'utilisation de drones équipés d'une caméra fait naître un risque élevé pour les droits et les libertés des personnes physiques et que, dès lors, il revenait au ministère de l'Intérieur de réaliser une analyse d'impact relative à la protection des données à caractère personnel »[475]. Elle relève trois manquements du ministère de l'Intérieur à la LIL révisée à savoir un défaut d'information des personnes concernées, l'absence d'une analyse d'impact sur la protection des données préalable à tout traitement de données par les forces de l'ordre ainsi qu'un traitement illicite (aucune disposition concernant l'usage de drones par les forces de l'ordre n'ayant été adoptée). La CNIL a donc émis un rappel à l'ordre à l'intention du ministre de l'Intérieur suivi d'une injonction de mettre en conformité les traitements concernés et a rendu publique sa décision.

188. En définitive, le Conseil d'État s'est prononcé à deux reprises (dans un arrêt du 18 mai 2020[476] puis dans un arrêt du 22 décembre 2020[477]) à l'encontre des forces de l'ordre de Paris afin de faire cesser sans délai l'emploi de drones de surveillance tant qu'aucun dispositif législatif adéquat n'aurait été adopté compte tenu du caractère fortement controversé et des incidences sur l'exercice des droits et libertés. Ces exemples soulignent la fragilité des droits et libertés face à la suprématie sécuritaire imposée par l'État s'appuyant en majeure partie sur les facilités que procurent les outils technologiques. La simplicité du point de vue technique que présente le déploiement des drones aériens agit indéniablement en faveur d'une utilisation par les forces de l'ordre et leur a permis de faire fi des injonctions du Conseil d'État et des recommandations de la CNIL de mettre fin à tout usage de cette technologie à des fins de surveillance.

---

[474] *Idem*, §17.

[475] *Idem*, §46.

[476] CE, ord., 18 mai 2020, n°440442, *op. cit.*

[477] CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155, *op. cit.*

B. L’échec de la loi pour une sécurité globale préservant les libertés

189. Depuis 2010, le ministère de l’Intérieur fait état d’une augmentation du nombre des manifestations de grande ampleur[478] et a, en outre, constaté que certains de ces mouvements avaient donné lieu à des atteintes à l’ordre public[479]. Ces constats ont attisé l’intérêt des forces de l’ordre d’avoir recours à des drones aériens afin d’améliorer la surveillance de la voie publique et la prévention des atteintes à l’ordre public, notamment lors de ces grands rassemblements. Cette technologie s’est également révélée particulièrement attrayante quant à ses potentialités de couplage avec des systèmes dits « intelligents » (en d’autres termes des algorithmes d’analyse d’évènements) ayant pour finalités de permettre la détection automatisée d’objets abandonnés ou de mouvements de foule[480] ou encore de comportements violents[481].

190. Les usages croissants des drones aériens par les forces de l’ordre et les services de secours se sont rapidement vus confrontés à l’absence d’encadrement répondant précisément aux enjeux juridiques qu’ils présentent[482]. Face à ce constat, le législateur a tenté une première fois d’encadrer ces pratiques au travers de plusieurs dispositions de la loi du 25 mai 2021 pour une sécurité globale préservant les libertés[483]. D’une manière générale, cette loi avait pour objectif d’attribuer aux forces de l’ordre « des moyens et des ressources pour assurer plus efficacement et

---

[478] Pour exemple, quelqu’uns des plus grands mouvements de manifestations depuis 2010 : le « Mouvement social sur les retraites » en 2010 (rassemblant *a minima* 2 millions de participants) ; le « Mariage pour tous » en mars 2013 ; la « Marche Républicaine » en janvier 2015 (réunissant *a minima* 3,7 millions de participants au lendemain des attentats de Charlie-Hebdo) ; le mouvement social et politique des « Gilets jaunes » en 2018 qui donna lieu à de nombreux affrontements, violences (des manifestants et des forces de l’ordre) et dégradations.
Voir sur ces sujets : Les archives du ministère de l’Intérieur [en ligne] ; « Les 10 plus grandes manifestations en France depuis 15 ans », *Le Nouvel Obs*, 8 septembre 2010 [en ligne] ou encore les « Archives des manifestations de France 24 », *france24.com* [en ligne] (consultés le 30 décembre 2022).

[479] PAUVERT (B.), « L’utilisation des drones à l’appui de la sécurité », *op. cit.*

[480] Voir en ce sens les travaux effectués dans le cadre des projets : ANR Flash GIRAFE développement d’algorithmes d’analyse situationnelle à l’usage des caméras fixes (mouvements de foule, détection de bagages abandonnés, détection et suivi d’individus suspects) pour les JOP 2024 [en ligne] ; FUI COOPOL développement de drones aériens à destination des forces de l’ordre et des services de secours de Paris équipés d’algorithmes de détection automatisée de comportements suspects, de suivi d’individus suspectés d’avoir commis une infraction, de détection de personnes dans un milieu enfumé et de reconstitution 3D d’un bâtiment [en ligne] ; ANR S2UCRE développement de caméras de surveillance (fixes et mobiles) et d’algorithmes d’analyse situationnelle (mouvements de foule et détection de comportements suspects) en milieu urbain à destination des forces de l’ordre [en ligne].

[481] PAUVERT (B.), « L’utilisation des drones à l’appui de la sécurité », *op. cit.*

[482] AN, Proposition de loi n°3452 relative à la sécurité globale, présenté par FAUVERGUE (J-M.) et THOUROT (A.) le 20 octobre 2020 [en ligne].

[483] Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*

plus simplement les missions qui leur sont confiées »[484]. Elle vient concrétiser l'objectif principal énoncé dans le *Livre blanc de la sécurité intérieure* de 2020 de « porter le ministère de l'Intérieur à la frontière technologique »[485]. En ce sens, la loi avait pour vocation de dépasser les propositions émises dans le rapport parlementaire sur la sécurité globale de 2018[486] en favorisant le recours à de nouveaux moyens technologiques par les forces de l'ordre, à l'image des drones aériens ou des caméras-piéton, en prévision notamment de la la Coupe du monde de rugby de 2023 et des Jeux Olympiques et Paralympiques (JOP) de 2024[487]. En vérité, la loi pour une sécurité globale vient asseoir cette ambition non dissimulée du gouvernement de mettre en œuvre un *continuum* de sécurité reposant sur l'usage de technologies de surveillance[488]. Ces dispositions visaient à introduire les nouveaux dispositifs (caméras mobiles et drones aériens équipés de caméras) et usages des caméras filmant la voie publique dans la législation relative à la vidéoprotection. La loi pour une sécurité globale entendait ainsi octroyer de nouvelles prérogatives aux forces de l'ordre et répondre à la demande formulée par les défenseurs des droits et libertés d'adapter la réglementation aux nouveaux cas d'usage de la vidéoprotection (1). Cependant, les dispositions relatives aux drones aériens furent rejetées par le Conseil constitutionnel, estimant qu'elles ne présentaient pas suffisamment de garanties à l'exercice des droits et libertés et déclarant une inconstitutionnalité partielle de la loi (2).

1. Une première tentative d'encadrement juridique des drones aériens de sécurité publique

191. Parmi les différentes technologies de surveillance traitées par la loi pour une sécurité globale, le législateur avait essentiellement pour objectif de donner une base légale plus adaptée aux drones aériens à l'usage des forces de l'ordre. Pour ce faire, il avait doté le texte de loi d'un volet dont les dispositions visaient à encadrer de manière spécifique les drones aériens en tant qu'outils

---

[484] AN, Proposition de loi n°3452 relative à la sécurité globale, *op. cit.*

[485] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*, p. 37.

[486] Rapport de la mission Parlementaire, « D'un *continuum* de sécurité vers une sécurité globale » remis par THOUROT (A.) et FAUVERGUE (J-M.), *op. cit.*

[487] AN, Proposition de loi n°3452 relative à la sécurité globale, *op. cit.*

[488] CLUZEL-MÉTAYER (L.), « Les aspects numériques de la loi pour la sécurité globale ou l'avènement de la "technosurveillance globale" », p. 103 *in* GALLOIS (J.) et MUREL (R.) (dir.), *La sécurité globale. Perspectives juridiques & éthiques*, *op. cit.*

de vidéoprotection sous l'appellation de « caméras aéroportées »[489]. L'article 47 de cette loi entendait insérer un nouveau chapitre dans le CSI intitulé « Caméras installées sur des aéronefs sans personne à bord » créant les articles L. 242-1 et suivants. Ces dispositions avaient pour vocation d'ouvrir un droit aux forces de l'ordre et aux services de secours de procéder au traitement d'images collectées au moyen d'un aéronef sans pilote à bord contrôlé par un télépilote[490]. Le législateur entendait étendre l'usage de la vidéoprotection aux drones aériens, qu'il s'agisse de missions de police administrative ou de police judiciaire.

192. Étant donné le caractère intrusif des drones aériens, le législateur avait prévu certaines garanties à leur recours par les forces de l'ordre afin de limiter leur incidence sur le droit à la vie privée, notamment en raison des données qu'ils peuvent collecter. Le législateur offrait une première garantie à l'usage des drones aériens de sécurité publique en interdisant la captation du son, l'analyse des images issues de leurs caméras au moyen de dispositifs automatisés de reconnaissance faciale, ainsi que les interconnexions, rapprochements ou mises en relation automatisés des DACP issues de ces traitements avec d'autres traitements de DACP[491]. Le législateur entendait ici prévenir les dérives liées à l'utilisation des systèmes de reconnaissance faciale et, dans le même temps, répondre à l'inquiétude des défenseurs des droits et libertés qui craignaient un usage généralisé de cette technologie entrainant un effet de surveillance de masse[492]. L'utilisation de cette technologie par deux lycées Marseillais avait suscité la réaction de la CNIL, qui l'avait jugée comme étant une mesure disproportionnée notamment du fait que d'autres mesures moins invasives étaient envisageables[493]. Saisi de l'affaire, le Tribunal administratif de Marseille

---

489 Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*, art. 47.

490 *Ibid*.

491 *Ibid*.

492 De manière non-exhaustive, voir notamment : CNIL, « Reconnaissance faciale - Pour un débat à la hauteur des enjeux », 15 novembre 2019, 11 p. [en ligne] ; European data Protection Board (EDPB), « EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination », June 21st 2021 [en ligne] ; Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), Lignes directrices sur « la reconnaissance faciale », 28 janvier 2021 [en ligne] ; DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », 19 juillet 2019 [en ligne] ; TOUATI (A.), NINO (G.), ELKOUBI (A.) et KOUM DISSAKE (V.), « La reconnaissance faciale, entre sécurité et droits fondamentaux », *Revue pratique de la prospective et de l'innovation* n° 2, 1er octobre 2019, p. 2 ; LEQUESNE ROTH (C.), « Interview de Caroline Lequesne sur la reconnaissance faciale dans l'espace public : bilan et perspectives européennes », *Dalloz IP/IT* n°6, 20 juin 2020, p. 332 ; Fablex DL4T, Rapport sur « Les usages européens de la reconnaissance faciale », avril 2020 [en ligne] ; « Le vrai visage de la reconnaissance faciale », *La Quadrature du Net*, 21 juin 2019 [en ligne].

493 CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », 29 octobre 2019 [en ligne].

était parvenu aux mêmes conclusions dans son jugement du 3 février 2020[494] rendant ainsi la première décision juridictionnelle sur ce sujet. L'initiative du Sénat d'interdire le recours à des dispositifs de reconnaissance faciale s'avérait donc particulièrement salutaire compte tenu du fait que cette technologie porte une atteinte significative aux droits et libertés et qu'aucune législation ne permet son utilisation à des fins de surveillance de la voie publique. En interdisant la captation du son par les drones aériens, le législateur s'était également efforcé d'éviter la censure du Conseil constitutionnel qui aurait sans doute jugé ces usages comme disproportionnés aux regards des finalités poursuivies.

193. Le texte tentait ensuite de répondre à l'obligation d'information du public quant au recours à ces dispositifs et aux personnels qui en sont responsables, énonçant qu'elle pouvait être effectuée « par tout moyen approprié »[495]. Cependant, cette disposition s'avérait trop évasive, le législateur n'ayant pas pris la peine d'apporter davantage de précisions quant aux « moyens » à mettre en œuvre. Cependant, le caractère aérien des drones rend précisément cette obligation d'information particulièrement complexe, notamment en comparaison d'autres systèmes de vidéoprotection[496]. De fait, les caméras disposées sur des drones aériens utilisés en milieu urbain se caractérisent par leur mobilité et leur discrétion. Ces caractéristiques sont la conséquence directe de leur miniaturisation, leur permettant de se mouvoir dans n'importe quel type d'environnement mais également d'avoir pour effet de les rendre « invisibles » aux yeux des personnes concernées qui seraient dès lors filmées à leur insu[497]. Aussi, la loi prévoyait plusieurs exceptions à cette obligation d'information lorsque les circonstances l'interdisaient ou dans le cas où cette mention d'information allait à l'encontre des objectifs poursuivis. Pour autant, cette obligation d'information demeure essentielle et les exceptions dont elle peut légitimement faire l'objet (telles que dans le cadre d'une enquête pénale) auraient méritées d'être explicitées dans le texte de loi.

194. Enfin, le texte de loi prévoyait deux autres garanties permettant un recours justifié à ces aéronefs par les forces de l'ordre et les services de secours. D'une part, la loi souhaitait garantir une

---

494 TA Marseille, 27 février 2020, n° 1901249, notamment §13 [en ligne].

495 Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*, art. 47.

496 Ceux-ci pouvant être facilement signalés par l'intermédiaire de panneaux informant les personnes de la présence de caméras ainsi que leurs droits s'agissant des données collectées les concernant.

497 La CNIL mettait en garde contre les risques pour les droits et libertés d'une généralisation du recours par les forces de l'ordre à des drones aériens par nature mobiles et discrets (CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, p. 3).

limitation temporelle de l'utilisation de drones aériens par les forces de l'ordre et les services de secours en exigeant une adaptation de cette durée en fonction des circonstances des missions[498]. Néanmoins, cette limitation manquait sensiblement de clarté et il aurait été opportun de fixer une durée en fonction des finalités pour lesquelles un drone aérien était employé, voire d'envisager dans quels cas et pour quelle durée il pouvait être justifié de prolonger son utilisation. D'autre part, le texte comprenait une garantie venant limiter les DACP pouvant être collectées à celles « strictement nécessaires à l'exercice des missions concernées », et exigeait dans le même temps le respect de la LIL[499]. Cette disposition se présentait comme venant en quelque sorte renforcer l'obligation de minimisation de la collecte des données par les forces de l'ordre. Par cette disposition plutôt rassurante, le législateur souhaitait démontrer sa volonté de renforcer l'obligation normalement applicable aux forces de l'ordre en matière de limitation des DACP pouvant être collectées. De fait, il est intéressant de noter que la formulation de cette disposition s'approche davantage de celle de l'article 5 du RGPD que de celle de l'article 4 de la DPJ, pourtant moins exigeante s'agissant du principe de minimisation de la collecte de DACP par les forces de l'ordre[500]. Pour autant, ces dispositions ne seront finalement pas promulguées suite à la décision rendue par le Conseil constitutionnel.

2. L'inconstitutionnalité partielle de la loi pour une sécurité globale

195. Le texte de loi fut soumis au contrôle du Conseil constitutionnel le 20 mai 2021 afin d'examiner notamment les dispositions relatives au recours à des drones aériens par les forces de l'ordre et les services de secours[501]. Cependant, la décision rendue par les Sages n'aura pas permis à ces dispositions d'être définitivement promulguées. Le Conseil constitutionnel avait frappé le texte d'inconstitutionnalité partielle notamment en raison des dispositions visant précisément à encadrer l'usage des drones aériens à des fins de vidéoprotection. Les Sages avaient appuyé leur décision sur deux critiques majeures de ces dispositions. En premier lieu, le manque de clarté des dispositions

---

498 Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*, art. 47.

499 *Ibid*.

500 De fait, l'article 5 §1, c) du RGPD énonce que « les données à caractère personnel doivent être […] limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » (en vertu du principe de minimisation des données) tandis que l'article 4 §1 c) de la DPJ exige seulement que les données à caractère personnel soient « non excessives au regard des finalités pour lesquelles elles sont traitées ».

501 C. cons., Décision n° 2021-817 DC, 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, *op. cit.*

relatives aux drones aériens de vidéoprotection qu'invoquaient les requérants[502]. En deuxième lieu et de manière générale, le juge constitutionnel avait estimé que compte tenu du caractère intrusif de ces dispositifs, ces dispositions ne permettaient pas d'assurer la nécessaire conciliation entre les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, d'une part, et le respect des droits et libertés de chacun, d'autre part[503].

196. Tout d'abord, le Conseil constitutionnel a rejeté les dispositions relatives au champ d'application des drones aériens de sécurité publique au motif que les différents contextes d'utilisation n'étaient pas suffisamment précis pour circonscrire leur utilisation aux évènements définis de manière stricte. En d'autres termes, il a estimé que le législateur n'avait pas mis en œuvre de « garanties particulières de nature à sauvegarder le droit au respect de la vie privée »[504]. Le texte prévoyait, de fait, un champ d'application très étendu permettant aux forces de l'ordre d'avoir recours à des drones aériens de sécurité publique afin de lutter contre « toute infraction, y compris pour une contravention »[505]. Ensuite, le Conseil constitutionnel a reproché au législateur de n'avoir prévu aucune garantie permettant de limiter la durée maximale de l'autorisation requise à l'usage de ces aéronefs par les forces de l'ordre[506]. En outre, il a estimé que le recours à des drones aériens ne présentait pas « un caractère subsidiaire en matière de police administrative »[507]. Enfin, les Sages ont estimé que les dispositions examinées n'assuraient pas le principe d'un contingentement permettant de limiter le nombre des aéronefs employés lors des missions[508] et ne prenaient pas suffisamment en compte les aspects relatifs à la protection de la vie privée et des données à caractère personnel[509].

---

[502] *Idem*, cons. 130.

[503] *Idem*, cons. 141

[504] *Idem*, cons. 135.

[505] *Idem*, cons. 137.

[506] *Idem*, cons. 138.

[507] *Idem*, cons. 139.

[508] *Idem*, cons. 140. À ce sujet, le professeur Serge Slama faisait remarquer que cette décision du Conseil constitutionnel entendait probablement prévenir l'utilisation de drones aériens en essaim comme le pratiquait déjà le ministère de la Défense (SLAMA (S.), « Censure partielle de la loi « sécurité globale » : après demain les drones ? », *Leclubdesjuristes.com*, 10 juin 2021 [en ligne]).

[509] *Idem*, cons. 135 : « eu égard à leur mobilité et à la hauteur à laquelle ils peuvent évoluer, ces appareils sont susceptibles de capter, en tout lieu et sans que leur présence soit détectée, des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre ».

197. Le Conseil constitutionnel n'a conservé en définitive que deux des sept contextes d'utilisation initialement prévus, à savoir celui relatif aux activités de sécurité civile tenant à la prévention des risques naturels ou technologiques, d'une part, et celui du secours aux personnes et la lutte contre l'incendie[510], d'autre part. Cependant, la décision du Conseil constitutionnel ne s'opposait pas à la possibilité d'un recours à des drones aériens équipés de caméras par les forces de l'ordre ; elle ne faisait qu'encourager le législateur à adopter un encadrement de ces dispositifs plus protecteur des droits et libertés[511]. C'est ce qui a permis à ce dernier de soumettre une nouvelle version de ces dispositions moins d'un an après.

§2. L'adoption d'un cadre juridique spécifique à l'usage des drones aériens de sécurité publique : une protection illusoire des droits et des libertés

198. Afin de répondre aux exigences exprimées par le Conseil constitutionnel dans sa décision du 20 mai 2021, le législateur a révisé les dispositions qu'il avait initialement adoptées concernant les drones aériens de sécurité publique (caméras aéroportées) dans la loi du 25 mai 2021. Dans les premières versions du texte de la loi RPSI, le législateur n'entendait autoriser l'emploi de drones aériens qu'à des fins préventives[512]. Ce n'est que par la suite, que le texte introduira une autorisation de leur usage à des fins répressives[513]. La loi RPSI du 24 janvier 2022 a permis de faire entrer

---

[510] CSI, art. L. 242-6.

[511] C. cons., Décision n° 2021-817 DC, 20 mai 2021, Loi pour une sécurité globale préservant les libertés, *op. cit.*, cons. 135 : le recours à des drones aériens peut être justifié « pour répondre aux objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions » ; SLAMA (S.), « Censure partielle de la loi « sécurité globale » : après demain les drones ? », *op. cit.* ; CLUZEL-MÉTAYER (L.), « Les aspects numériques de la loi pour la sécurité globale ou l'avènement de la "technosurveillance globale" », p. 109 *in* GALLOIS (J.) et MUREL (R.) (dir.), *La sécurité globale. Perspectives juridiques & éthiques*, *op. cit.* ; BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *op. cit.*

[512] AN, Projet de loi n°4387 relatif à la responsabilité pénale et à la sécurité intérieure, présenté par DUPONT-MORETTI (É.) et DARMANIN (G.) le 20 juillet 2021, art. 8 [en ligne].

[513] BOUCHET (M.), « Décollage pour l'utilisation des drones par les policiers et gendarmes », *Gaz. Pal.* n°40, 16 novembre 2021, p. 12.

définitivement dans le droit commun les drones aériens de sécurité publique qui bénéficient désormais d'un cadre juridique spécifique[514] comme outil de vidéoprotection.

199. Les usages technologiques, qui semblent désormais faire loi, contraignent le législateur à instaurer de nouvelles règles juridiques adaptées à chaque type de technologie. Les drones aériens de sécurité publique n'ont pas fait exception. La loi RPSI permet l'usage de drones aériens par les policiers et gendarmes nationaux sous réserve de l'obtention préalable d'une autorisation de mise en œuvre et dans des conditions d'usage strictement définies. En révisant les dispositions initiales issues de la loi pour une sécurité globale, le législateur a voulu renforcer les garanties entourant l'usage des drones aériens par les forces de l'ordre (A). Ces garanties semblent néanmoins fragiles eu égard aux contraintes que portent les drones aériens de sécurité publique aux droits et aux libertés, particulièrement lorsqu'ils sont utilisés dans le cadre de la procédure pénale[515]. En ce sens, le suivi d'une personne circulant sur la voie publique par un drone aérien utilisé par les forces de l'ordre pourrait porter atteinte à son droit au respect de la vie privée ainsi qu'à ses données personnelles voire à sa liberté d'aller et venir. De même, la captation d'images par drone aérien lors d'une manifestation est susceptible d'avoir une incidence sur la liberté d'expression et d'opinion des participants en suscitant leur méfiance et en limitant sensiblement leurs agissements[516] (B).

---

[514] La loi crée « une base légale spécifique pour l'usage de caméras aéroportées par les forces de sécurité intérieure, en prenant compte les objections énoncées par le Conseil constitutionnel » telle que l'entendait le Sénat dans son Rapport n°46 (2021-2022) par JOURDA (M.) et HERVÉ (L.), Projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, *op. cit.*, p. 60. Ce cadre a par la suite été précisé lors de la publication du décret n° 2023-283 du 19 avril 2023 relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs pour des missions de police administrative (*JORF* n°0093 du 20 avril 2023 [en ligne]) et de l'arrêté du 19 avril 2023 relatif au nombre maximal de caméras installées sur des aéronefs pouvant être simultanément utilisées dans chaque département et collectivité d'outre-mer (*JORF* n°0093 du 20 avril 2023 [en ligne]) après délibération de la CNIL Délibération n° 2023-027 du 16 mars 2023 portant avis sur un projet de décret portant application des articles L. 242-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs par les services de la police nationale, de la gendarmerie nationale, des douanes ainsi que les militaires des armées déployés sur le territoire national dans le cadre des réquisitions prévues à l'article L. 1321-1 du code de la défense (demande d'avis n° 22015146) RU n° 72, *JORF* n°0093 du 20 avril 2023 [en ligne]).

[515] BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *op. cit.*

[516] Voir par exemple : CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 99 : « un drone est susceptible d'affecter le comportement des personnes qui ont perçu sa présence, l'objectif est de collecter des informations, non d'affecter son environnement » (traduit de l'anglais).

A. Les conditions du recours aux drones aériens de sécurité publique

200. Dans sa décision du 21 janvier 2022[517], le Conseil constitutionnel a autorisé le renforcement des pouvoirs de prévention des atteintes à l'ordre public et de constatation des infractions des forces de police et de gendarmerie nationales. En dépit des nombreuses critiques qu'il avait formulées à l'encontre des dispositions relatives à l'usage des drones aériens issues de la loi de 2021, le Conseil constitutionnel ne s'était pas opposé à l'octroi d'un recours à cette technologie par les forces de l'ordre. Le législateur a donc soumis de nouvelles dispositions tenant compte des réflexions formulées par le Conseil. Les dispositions de la loi RPSI diffèrent ainsi sensiblement de celles issues de la loi pour une sécurité globale préservant les libertés en ce qu'elles distinguent clairement le recours à des drones aériens à des fins de police administrative (dont les dispositions sont inscrites dans le CSI) de leur recours à des fins de police judiciaire (dont les dispositions ont été intégrées dans le CPP). La loi comporte également des garanties renforcées pour les droits et libertés s'efforçant de répondre à l'exigence de clarté de ses dispositions. Elle introduit des conditions strictes de mise en œuvre (1) et d'utilisation (2) des drones aériens par les forces de l'ordre.

1. Les conditions d'autorisation du recours aux drones aériens de sécurité publique

201. La loi introduit de nouvelles dispositions dans le CSI autorisant les policiers et gendarmes nationaux à recourir à des drones aériens équipés de caméras afin de capter, enregistrer et transmettre des images « dans l'exercice de leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens »[518]. Aussi, elle ouvre au sein du CPP un droit similaire aux policiers et aux gendarmes nationaux dans les cas où cela serait nécessaire aux fins d'enquête, d'instruction ou d'information[519]. La loi RPSI soumet le recours à des drones aériens de sécurité publique à une autorisation (a) et délimite leur champ temporel et spatial d'action (b).

---

[517] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.* ; *AJDA* 2022 p. 127, obs. MAUPIN (E.) ; *AJCT* 2022 p. 66, obs. ROYER (E.) ; *Dalloz IP/IT* 2022 p.63, obs. CRICHTON (C.)

[518] CSI, art. L. 242-5, I.

[519] CPP, art. 230-47 et suiv. ; art. 74, 74-1 art. 74-2 et 80-4.

a. Des prérogatives soumises à l'autorisation d'une autorité compétente

202. Le texte diffère de la version de 2021 s'agissant des nouvelles prérogatives accordées aux policiers et aux gendarmes nationaux dans la mesure où le législateur est venu préciser l'autorité compétente pour délivrer l'autorisation exigée en accord avec la nature de l'activité relevant soit de la police judiciaire soit de la police administrative. L'autorisation relève ainsi de la compétence du juge d'instruction ou du procureur de la République[520] en matière de police judiciaire. Toutefois, en matière de police administrative, le texte précise que l'autorisation, délivrée par le préfet territorialement compétent, doit être écrite et motivée[521].

203. Le législateur est venu délimiter les pouvoirs confiés aux policiers et aux gendarmes nationaux quant à l'usage qu'ils peuvent faire des drones aériens en définissant les différentes finalités pour lesquelles ils peuvent être mis en œuvre[522]. Le texte de loi reprend six des sept finalités qui avaient été proposées dans la loi de 2021[523]. Néanmoins, celles-ci ressemblent à s'y méprendre à celles prévues à l'usage des caméras fixes de vidéoprotection. Ainsi, le caractère prétendument adapté des dispositions relatives à l'emploi de drones aériens laisse quelque peu perplexe compte tenu de la nature très intrusive de cette technologie[524] dont l'usage aurait mérité

---

[520] CPP, art. 74 à 74-2 et 230-48.

[521] CSI, art. L. 242-5, IV, al. 10 et 11 : L'autorisation devra préciser « la finalité poursuivie [qui] ne peut excéder le périmètre géographique strictement nécessaire à l'atteinte de cette finalité » ainsi que « le nombre maximal de caméras pouvant procéder simultanément aux enregistrements, au regard des autorisations déjà délivrées dans le même périmètre géographique ». Ce dernier point avait précisément donné lieu à des critiques du juge constitutionnel qui avait reproché au législateur d'avoir omis de préciser le nombre de dispositifs pouvant être simultanément mis en œuvre lorsqu'il avait soumis le texte au contrôle de constitutionnalité en 2021. Il vient ainsi répondre aux exigences émises par le Conseil constitutionnel.

[522] CSI, art. L. 242-5, I et II, et CPP, art. 230-47.

[523] Le texte ne reprend pas la finalité correspondant à « la protection des bâtiments et installations publics et de leurs abords immédiats, lorsqu'ils sont particulièrement exposés à des risques d'intrusion ou de dégradation » inscrite (art. 47 introduisant l'article L. 242-5, II) dans la Proposition de loi n°599 adoptée par l'Assemblée nationale pour une sécurité globale préservant les libertés du 15 avril 2021 [en ligne].

[524] Voir en ce sens : CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, pp. 3-4 : Les drones aériens constituent des « dispositifs mobiles, discrets par nature et dont la position en hauteur leur permet de filmer des lieux jusqu'ici difficiles d'accès voire interdits aux caméras classiques. La captation d'images qu'ils permettent est donc considérablement élargie et, surtout, peut être individualisée, en permettant le suivi de personnes dans leurs déplacements, à leur insu et sur une durée qui peut être longue. En outre, davantage que les caméras actuellement utilisées, ces dispositifs de surveillance sont susceptibles d'influer sur l'exercice par les citoyens d'autres libertés fondamentales » ; C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.*, cons. 135 : Le juge constitutionnel avait relevé qu'« eu égard à leur mobilité et à la hauteur à laquelle ils peuvent évoluer, ces [drones aériens] sont susceptibles de capter, en tout lieu et sans que leur présence soit détectée, des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre » ; BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *Procédures* n°6, juin 2022, pp. 11-15, spéc. p. 14 : Dans son étude, le professeur Jacques Buisson avait qualifié leur emploi de « moyen particulièrement intrusif ».

d'être limité à des situations exceptionnelles. Les finalités trop extensives qui pouvaient déjà être reprochées au cadre prévu pour les caméras fixes de vidéoprotection, à l'image de « la prévention d'actes de terrorisme »[525], ont donc été malheureusement reprises s'agissant des drones aériens de sécurité publique.

204. Soucieux du contrôle du Conseil constitutionnel, le législateur s'est efforcé de préciser les conditions dans lesquelles les différentes finalités pouvaient être remplies en exigeant que le recours à des drones aériens de sécurité publique ne puisse « être uniquement autorisé [que] lorsqu'il est proportionné au regard de la finalité poursuivie »[526]. Cependant, cette précision n'a pas été jugée comme suffisamment protectrice des droits et libertés par le Conseil constitutionnel s'agissant du cadre de la police administrative. Les Sages ont donc formulé une réserve d'interprétation concernant la délivrance par le préfet des autorisations d'emploi de drones aériens. Celle-ci exigeait que le préfet s'assure que les forces de l'ordre ne puissent « employer de moyens moins intrusifs au regard de ce droit ou que l'utilisation de ces autres moyens serait susceptible d'entrainer des menaces graves pour l'intégrité physique des agents »[527].

205. Par la suite, la délibération de la CNIL du 16 mars 2023 concernant le projet de décret d'application des articles du CSI relatifs à l'usage de caméras aéroportées par les forces de l'ordre avait pris note de la décision des ministères concernés de mettre en œuvre une doctrine d'emploi propre à chacune des institutions concernées (police nationale, gendarmerie nationale, militaires et douanes). Aussi, la CNIL avait constaté la difficulté de « définir dans le projet de décret des critères objectifs encadrant la captation, l'enregistrement et la transmission d'images »[528] et avait estimé, en conséquence, que ces précisions devraient être mentionnées dans la doctrine d'emploi qui devrait lui être communiquée préalablement à toute utilisation.

---

[525] Cette finalité, de par son champ illimité, se révèle particulièrement complexe à définir (HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 350 : « La définition juridique du terrorisme soulève des difficultés »).

[526] CSI, art. L. 242-5, I, dernier al.

[527] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, *op. cit.*, cons. 27 : « Une telle autorisation ne saurait cependant, sans méconnaître le droit au respect de la vie privée, être accordée qu'après que le préfet s'est assuré que le service ne peut employer d'autres moyens moins intrusifs au regard de ce droit ou que l'utilisation de ces autres moyens serait susceptible d'entraîner des menaces graves pour l'intégrité physique des agents ».

[528] CNIL, Délibération n° 2023-027 du 16 mars 2023, *op. cit.*

b. Des prérogatives limitées dans le temps et dans l'espace

206. Tenant compte des critiques formulées par le Conseil constitutionnel en 2021, le législateur a renforcé les garanties concernant la limitation temporelle de l'utilisation des drones aériens par les forces de l'ordre. Cette fois, le législateur a précisé la durée maximale de l'autorisation d'utilisation de drones aériens de vidéoprotection qui n'est délivrée que pour une durée de trois mois renouvelable s'agissant des activités de police administrative[529]. Aussi, cette durée fait l'objet d'une exception lorsqu'il s'agit d'assurer la sécurité d'un rassemblement de personnes puisque leur utilisation est limitée à la durée du rassemblement. Ici encore, le Conseil constitutionnel a tenu à renforcer les garanties prévues par la loi en formulant une autre réserve constitutionnelle exigeant que le préfet ne puisse renouveler leur utilisation « sans qu'il soit établi que le recours à ces dispositifs aéroportés demeure le seul moyen d'atteindre la finalité poursuivie »[530].

207. S'agissant des activités relevant de la police judiciaire, l'autorisation reste délivrée par un magistrat mais le législateur précise ici aussi la durée maximale pour laquelle ces dispositifs peuvent être utilisés[531]. Ainsi, le texte répond aux recommandations émises par le Conseil d'État d'exiger l'autorisation d'un magistrat délivrée pour une courte durée[532] en application de l'interprétation jurisprudentielle de la Cour de cassation[533]. Dans le cadre d'une enquête préliminaire ou de flagrance, l'autorisation relève de la compétence du procureur de la République et est limitée à une durée d'un mois renouvelable une fois[534]. Dans le cadre d'une instruction, l'autorisation est délivrée par le juge d'instruction pour une durée maximale de quatre mois renouvelables dans la limite de deux ans[535]. Le texte répond dès lors aux exigences formulées par le

---

529 CSI, art. L. 242-5, IV.

530 C. const., Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, *op. cit.*, cons. 28.

531 CPP, art. 230-48.

532 CE, Avis n° 401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, 20 septembre 2020, *op. cit.*, p. 5.

533 Concernant l'interprétation de la Cour de cassation s'agissant des dispositions du CPP relatives à la procédure de constitution de preuves d'une infractions permettant d'identifier des personnes par un dispositif de captation d'images de la voie publique : C. cass., ch. crim., 11 décembre 2018, n°18-82.365 [en ligne] et C. cass., ch. crim., 18 juin 2019, n°18-86-421 [en ligne].

534 CPP, art. 230-48 1°.

535 CPP, art. 230-48 2°.

Conseil constitutionnel en précisant que dans tous les cas, la décision d'autorisation délivrée par le magistrat devra comporter des éléments précisant la durée du recours à ces aéronefs[536].

208. La loi RPSI comporte également des limites spatiales qui, à l'instar d'autres systèmes de vidéoprotection, interdisent la captation d'images « de l'intérieur des domiciles [ou], de façon spécifique, celles de leurs entrées »[537]. Aussi, le texte prévoit que lorsque cette condition n'a pas été respectée, l'enregistrement doit être immédiatement interrompu ou à défaut (lorsque des circonstances exceptionnelles ne le permettent pas) supprimé dans les quarante-huit heures à compter de la fin du recours au dispositif de vidéoprotection[538].

209. Ce pouvoir intrusif permettant la constatation d'infractions par l'intermédiaire de drones aériens de sécurité publique a toutefois été soumis à des conditions précises par le Conseil constitutionnel, qui l'a limité aux seuls agents de la police et de la gendarmerie nationales[539]. De fait, il a déclaré comme inconstitutionnelles les dispositions visant à autoriser provisoirement la police municipale à capter et enregistrer des images au moyen de drones aériens équipés de caméras afin d'assurer la régulation des flux de transport, les mesures d'assistance et de secours aux personnes, la sécurité des manifestations sportives, récréatives ou culturelles[540].

210. Les Sages formulaient trois reproches à ces dispositions. En premier lieu, ils estimaient que « le législateur a permis à ces services de recourir à ces dispositifs aéroportés […] sans limiter cette dernière finalité aux manifestations particulièrement exposées à des risques de troubles graves à l'ordre public »[541]. En deuxième lieu, ils reprochaient au législateur de ne pas avoir limité la durée d'emploi de ces dispositifs en permettant au préfet qui accorde l'autorisation de mettre fin à leur recours « à tout moment, dès lors qu'il constate que les conditions ayant justifié sa délivrance ne sont plus réunies »[542]. Enfin, le Conseil constitutionnel constatait l'imprécision des dispositions

---

[536] CPP, art. 230-49.

[537] CSI, art. L. 242-5, III.

[538] *Idem*.

[539] Ainsi qu'aux militaires des armées exerçant leur activité sur le territoire national par réquisition (Code de la défense, art. L. 1321-1).

[540] Loi RPSI, art. 15, 8° et CSI, art. L. 242-7.

[541] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 35.

[542] *Idem*, cons. 36.

relatives à l'emploi par la police municipale - sans autorisation du préfet[543] - de drones aériens en cas d'urgence[544]. En conséquence, il a censuré les dispositions du 8° de l'article 15 du texte, estimant qu'elles ne permettaient pas d'assurer une conciliation équilibrée entre l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, d'une part, et le droit au respect de la vie privée protégé par l'article 2 de la DDHC de 1789[545], d'autre part. Aussi, le Conseil constitutionnel a déclaré contraire à la Constitution de 1958 les dispositions permettant l'utilisation en cas d'urgence de drones aériens par les policiers et gendarmes nationaux sans autorisation préalable du préfet pour une durée pouvant aller jusqu'à quatre heures[546].

211. Le législateur a soumis à l'octroi d'une autorisation par les autorités compétentes le recours à des drones aériens par les policiers et gendarmes nationaux et complété cette obligation de plusieurs garanties conditionnant leur déploiement. Ces garanties ont été quelque peu précisées dans le décret et l'arrêté du 19 avril 2023[547]. Le décret indique les conditions de l'autorisation de recourir à des caméras aéroportées par l'envoi préalable d'un engagement de conformité aux dispositions du CSI y afférents[548]. Aussi, il énumère les différentes personnes pouvant avoir accès aux données collectées par ces dispositifs[549]. L'arrêté précise enfin le nombre de caméras aéroportées[550] pouvant être simultanément déployées par les forces de l'ordre.

2. Les conditions d'emploi des drones aériens de sécurité publique

212. À la lumière des considérants issus de la décision du 20 mai 2021 et tenant compte de leurs incidences sur les droits et libertés, le législateur a dû encadrer strictement le recours aux

---

[543] La disposition prévoyait une durée d'emploi des drones aériens pouvant atteindre quatre heures et soumis à la seule condition d'avoir informé le préfet au préalable (Loi RPSI, art. 15, 8°).

[544] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 37.

[545] *Idem*, cons. 38.

[546] *Idem.*, cons. 31 : « Les dispositions contestées prévoient que, en cas d'urgence résultant d'« une exposition particulière et imprévisible à un risque d'atteinte caractérisée aux personnes ou aux biens », ces mêmes services peuvent recourir immédiatement à ces dispositifs aéroportés, pour une durée pouvant atteindre quatre heures et à la seule condition d'en avoir préalablement informé le préfet. Ainsi, ces dispositions permettent le déploiement de caméras aéroportées, pendant une telle durée, sans autorisation du préfet, sans le réserver à des cas précis et d'une particulière gravité, et sans définir les informations qui doivent être portées à la connaissance de ce dernier ».

[547] DE MONTECLER (M-C.), « Ô drone, reprends ton vol ! », *AJDA* n° 16, 1er mai 2023, p. 813.

[548] Décret n° 2023-283 du 19 avril 2023, *op. cit.*, art. 2 et CSI, art. R. 242-14.

[549] Décret n° 2023-283 du 19 avril 2023, *op. cit.*, art. 2 et CSI, art. R. 242-10.-I.

[550] Celui-ci diffère sensiblement selon le département ou la collectivité territoriale concernée (entre 40 et 100).

drones aériens de sécurité publique. Il avait donc entrepris de renforcer l'obligation d'information à laquelle sont tenues les forces de l'ordre dans le cadre de l'emploi d'un dispositif de vidéoprotection. Le texte indique que le public peut être informé par tout moyen de l'emploi de ces dispositifs ainsi que de l'autorité qui en est responsable[551] et précise qu' « une information générale du public sur l'emploi de dispositifs aéroportés de captation d'images est organisée par le ministre de l'intérieur »[552]. Dès lors, le législateur n'apporte toujours aucune précision quant aux moyens ou aux circonstances permettant de délivrer cette information générale au public quant à l'emploi temporaire de drones aériens par les forces de l'ordre. Or, étant donné que des DACP seront collectées par ces dispositifs, la réglementation relative à la protection des données personnelles exige que le public soit informé du traitement de leurs données en vertu du principe de loyauté et de la transparence de la collecte[553].

213. La loi RPSI reprend les dispositions du texte initial visant un encadrement strict de la collecte des données par les drones aériens utilisés par les forces de l'ordre. Le législateur maintient par conséquent son exigence limitant la collecte des données à celles « strictement nécessaires à l'exercice des missions concernées » et adaptées selon les circonstances de chaque mission dans le respect de la règlementation relative à la protection des données[554]. Aussi, il rappelle qu'au même titre que les caméras fixes de vidéoprotection, le traitement de DACP par les drones aériens de sécurité publique fera préalablement l'objet d'un « décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés »[555]. En outre, il renouvelle son interdiction à l'encontre des forces de l'ordre d'avoir recours à des drones aériens afin de procéder à la captation de sons ou de faire usage de traitements automatisés de reconnaissance faciale. Il conserve également l'interdiction de procéder au rapprochement, à l'interconnexion ou à la mise en relation automatisée avec d'autres traitements de DACP[556].

---

[551] CSI, art. L. 242-3 : « Le public est informé par tout moyen approprié de l'emploi de dispositifs aéroportés de captation d'images et de l'autorité responsable de leur mise en œuvre, sauf lorsque les circonstances l'interdisent ou que cette information entrerait en contradiction avec les objectifs poursuivis ».

[552] *Idem*.

[553] En matière de police administrative et de police judiciaire respectivement : DPJ, art. 5 et art. 13.

[554] CSI, art. 242-4, al. 1er.

[555] CSI, art. 242-8.

[556] CSI, art. 242-4, al. 2.

214. Le Conseil constitutionnel a admis ces dispositions en les complétant toutefois d'une réserve d'interprétation estimant qu'elles « ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés »[557]. Par cette réserve d'interprétation, les Sages ont exprimé leur méfiance quant à l'usage, sous toutes ses formes, de la reconnaissance faciale qui demeure le sujet de fortes controverses. Toutefois, il peut être reproché au législateur comme au Conseil constitutionnel d'avoir omis de prendre en compte d'autres types de systèmes automatisés de traitement de données, à l'image de ceux effectuant le suivi d'individus sans réidentification mais qui permettent une individualisation des personnes ou encore ceux collectant d'autres types de données biométriques telles que la démarche d'un individu. En ce sens, la haute juridiction n'a pas pleinement profité de ce second examen des dispositions afin d'anticiper de futures atteintes aux droits et libertés.

215. Les dispositions législatives fixent de nouvelles limites à la durée de conservation des enregistrements vidéo, selon qu'il s'agisse d'une activité de police administrative ou d'une activité de police judiciaire[558]. Ainsi, les enregistrements effectués dans le cadre d'une mission relevant de la police administrative ne sont conservés que durant sept jours après la fin de leur déploiement et leur accès est interdit à l'exception des cas de signalement par la police judiciaire[559]. Le législateur a sensiblement réduit la durée de conservation possible de ces enregistrements, passant d'une durée d'un mois (comme celle admise pour les caméras fixes de vidéoprotection) à une semaine. Cette restriction de la durée de conservation des enregistrements issus des drones aériens se justifie tant par leur caractère sensiblement intrusif pour la vie privée que par leur contexte d'utilisation, les caméras aéroportées ayant pour vocation de filmer de manière discontinue (à l'inverse des caméras fixes). Cette mesure mérite d'être saluée, le législateur ayant fait un effort concret afin d'adapter la durée de conservation des images aux usages des drones aériens par les forces de l'ordre. Aussi, il n'est pas surprenant de voir apparaitre une exception à cette mesure dans le cadre de l'ouverture d'une enquête judiciaire. Enfin, le législateur a maintenu la possibilité de transmettre en temps réel les données issues du drone aérien au poste de commandement permettant une pré-sélection des

---

[557] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 30.

[558] CSI, art. L. 242-4 et CPP, art. 230-53.

[559] CSI, art. L. 242-4, c).

images utiles à une éventuelle procédure judiciaire[560]. Les enregistrements effectués à des fins de police judiciaire sont, pour leur part, conservés jusqu'à l'expiration de l'action publique[561].

216. Enfin, la loi RPSI introduit des dispositions permettant de garantir la fiabilité des données, exigeant la mise en œuvre de dispositifs techniques permettant d'assurer l'intégrité des enregistrements[562] ainsi que la traçabilité des consultations des données[563]. À cette fin, le législateur impose à l'autorité compétente de tenir un registre des traitements mis en œuvre précisant la finalité poursuivie, la durée des enregistrements, les personnes ayant eu accès aux images, y compris en temps réel. Dans le cadre de la police judiciaire, les enregistrements des drones aériens sont « placés sous scellés fermés » afin de garantir la confidentialité des données[564].

217. Sur la question des drones aériens à l'usage des forces de l'ordre, le Conseil constitutionnel a partiellement censuré l'article 15 de la loi et émis plusieurs réserves d'interprétation. Ainsi, il a réalisé un contrôle relativement consciencieux des usages préventifs des drones aériens. En revanche, il s'est avéré nettement plus conciliant s'agissant du recours aux drones aériens dans le cadre des enquêtes pénales[565] en ne s'attardant que brièvement sur les dispositions afférentes aux usages à des fins de police judiciaire[566].

218. Le législateur ne s'est pas découragé dans sa quête d'apporter un cadre adapté aux drones aériens à l'usage des forces de l'ordre. Toutefois, malgré le contrôle préalable du Conseil constitutionnel, cette loi souffre encore de nombreuses lacunes pour adapter au mieux les usages de ces dispositifs au respect des droits et libertés. Il n'aura fallu qu'une seconde tentative (légèrement teintée de changements) au législateur pour que la Haute juridiction déclare les dispositions, relatives à l'usage des drones aériens par les forces de l'ordre, conformes à la Constitution, en dépit

---

[560] CSI, art. L. 242-2.

[561] CPP, art. 230-53.

[562] CSI, art. L. 242-2, al. 2.

[563] CSI, art. L. 242-4, al. 3.

[564] CPP, art. 230-52.

[565] Voir notamment : PELLÉ (S.), « De la responsabilité pénale, du trouble mental et de quelques dispositions en matière de sécurité intérieure », *Rec. Dalloz*, 2022, p. 519.

[566] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 40-47.

de garanties encore insuffisantes.

B. Des garanties fragiles à l'usage des drones aériens de sécurité publique

219. La loi RPSI a mis en œuvre plusieurs garanties permettant d'assurer la conciliation entre le respect des droits et libertés et le recours à des drones aériens de sécurité publique par les forces de l'ordre à des fins de prévention de l'ordre public et de recherche des auteurs d'infractions. Néanmoins, ces garanties semblent dérisoires au vu du caractère particulièrement intrusif lié à la captation et la transmission de données, principalement d'images, en temps réel par les drones aériens de sécurité publique. Cette technologie renforce indubitablement le pouvoir de contrainte exercé sur les individus par la surveillance de la voie publique.

220. L'emploi de drones aériens de sécurité publique dépasse de fait la « simple » prévention des infractions (comme le feraient d'autres systèmes de vidéoprotection) et conduit « à une recherche coercitive d'infractions »[567] par les agents de la police et de la gendarmerie nationales. En d'autres termes, la contrainte posée par cette technologie de surveillance ne se limite pas à la seule constatation d'une infraction qui pourrait advenir lors d'une intervention des forces de l'ordre mais repose sur une recherche de la commission d'une infraction dans le cadre d'une mission de police administrative. De ce fait, les missions de police administrative tendent à se confondre avec celles de police judiciaire[568]. Cette distinction essentielle entre la police judiciaire et la police administrative[569], qui souffrait déjà d'une forte atténuation[570], devrait d'autant plus s'estomper par le recours aux drones aériens de sécurité publique. Cela souligne un premier constat de la fragilité des

---

567 BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 13.

568 Pour rappel, la police administrative a pour mission d'assurer le maintien de l'orde public (missions préventives) tandis que la police judiciaire œuvre à la recherche des auteurs d'infractions (missions répressives).

569 GAUDEMET (Y.), *Droit administratif*, Paris, LGDJ, 23ème édition, 2020, 648 p., p. 388 : « La distinction de la police administrative et de la police judiciaire est une distinction importante dans la mesure où le contentieux de la police administrative relève de la juridiction administrative alors que le contentieux des activités de police judiciaire lui échappe et dans la mesure où, dans le domaine de la responsabilité, les dommages causés par les actes de police administrative sont susceptibles d'engager la responsabilité de l'administration avec une plus grande certitude que ceux qui peuvent résulter d'actes de police judiciaire ». Voir également en ce sens : BEAULAC (L.), La distinction police administrative - police judiciaire conserve-t-elle une utilité ?, Thèse, Université de Pau et des Pays de l'Adour, 2001, p. 389 ; GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 37.

570 De manière non-exhaustive : GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, spéc. pp. 189-255 ; PARIZOT (R.), « La distinction entre police administrative et police judiciaire est-elle dépassée ? », *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, pp. 133-145 ; HERRAN (T.), « L'impact de la loi relative à la sécurité publique sur la distinction entre la police judiciaire et la police administrative », *AJ Pénal* n° 11,16 novembre 2017, p. 472.

garanties de cette loi au vu du renforcement des contraintes que subit la procédure pénale. Ce sentiment de suspicion généralisée de la population que suscitent les drones aériens de sécurité publique vient ainsi bousculer le principe même de la présomption d'innocence, inhérent à la procédure pénale et au droit à la sûreté. Dès lors, la loi RPSI s'inscrit dans la continuité de la loi n°2015-912 du 24 juillet 2015 relative au renseignement[571] établissant le cadre de la police administrative matérielle[572] permettant le recours à une surveillance coercitive à des fins de recherche d'infractions[573]. La création de cette police administrative matérielle par la loi de 2015 avait déjà sensiblement affecté la frontière qui sépare encore la police administrative de la police judiciaire. Ainsi, en dépit de la volonté du législateur de distinguer les usages de drones aériens entre les activités de police administrative et celles de police judiciaire, le caractère particulièrement contraignant tenant à la recherche (et non plus seulement à la constatation) des infractions par cette technologie souligne la fragilité de cette distinction (v. **n° 570 et suiv.**).

221. Outre l'atténuation de la distinction entre police administrative et police judiciaire que suscitent les drones aériens de sécurité publique, ceux-ci disposent d'un cadre juridique dont les conditions d'autorisation (1) et d'emploi (2) ne permettent pas d'assurer la protection effective des droits et des libertés au regard de leurs particularités mobiles et aériennes.

1. Des conditions d'autorisation trop permissives à l'égard des drones aériens de sécurité publique

222. Une première critique peut être formulée s'agissant de l'étendue du champ des finalités permettant le recours à des drones aériens par les forces de l'ordre et les services de secours. Ces finalités, au nombre de six, ouvrent un spectre large d'action[574] similaire à celui des caméras fixes de vidéoprotection. Pourtant, les drones aériens se distinguent des caméras fixes par leurs particularités (hauteur de vol, mobilité et discrétion) ce qui aurait dû inciter le législateur à la prudence en limitant les recours possibles pour faire face à leur pouvoir hautement coercitif. En ce sens, l'avis du Conseil d'État du 20 septembre 2020 enjoignait le législateur à autoriser l'emploi de

---

571 Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n°0171 du 26 juillet 2015 [en ligne].

572 GUINCHARD (V. S.) et BUISSON (J.), *Procédure pénale*, Paris, LexisNexis, 15e édition, 2022, 1620 p., n° 676 et s.

573 BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 13.

574 Syndicat de la magistrature, « Observations sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure - Volet n°3 : dispositions relatives à la surveillance (Articles 7, 8, 9) », *op. cit.*, p. 7.

drones aériens de manière proportionnée et adaptée aux situations[575], notamment en concevant des dispositions « adaptées aux spécificités de certains modes de captation »[576]. Aussi, la CNIL rappelait que le recours à ces dispositifs était soumis à deux conditions cumulatives tenant à la stricte nécessité de leur utilisation et à la proportionnalité de leur mise en œuvre[577]. Elle craignait ainsi que la multiplication des finalités d'utilisation des drones aériens par les forces de l'ordre et les services de secours conduise à une banalisation de leur usage. Dès lors, elle exigeait que le recours à ces dispositifs soit limité dans le cadre de la prévention des atteintes à la sécurité des personnes et des biens « à la lutte contre les infractions d'un degré élevé de gravité »[578].

223. En dépit des recommandations émises tant par le Conseil d'État que par la CNIL, le législateur n'a pas pris en compte le besoin de limiter le nombre des infractions pouvant entrer dans le cadre d'une utilisation de drones aériens. Pire, le Conseil constitutionnel a fait preuve d'une grande souplesse à l'égard des usages des drones aériens dans le cadre des activités de police judiciaire. Le législateur avait pourtant révisé les dispositions qu'il avait adopté en 2021 concernant l'étendue du champ des infractions pour lesquelles les forces de l'ordre pouvaient faire usage de drones aériens. Néanmoins, la loi RPSI abaisse la peine encourue de cinq à trois ans d'emprisonnement des crimes et délits pouvant faire l'objet d'un recours à ces dispositifs[579]. Il s'ensuit qu'un nombre plus important d'infractions sont concernées par cette nouvelle forme de vidéoprotection, entrainant *de facto* une probabilité conséquente d'avoir recours à ces dispositifs et de voir imposer des restrictions plus importantes aux droits et libertés. Cependant, le principe de proportionnalité auquel sont soumis les dispositifs de vidéoprotection impose que la collecte des données soit limitée à celles nécessaires aux finalités poursuivies. Or, l'application effective de ce principe est sérieusement remise en question compte tenu du manque de démonstration lors des débats de la nécessité de faire usage de drones aériens à des fins de sauvegarde de l'ordre public, d'une part, et de l'étendue du champ des finalités permettant leur recours, d'autre part. La décision

---

[575] CE, Avis n° 401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, 20 septembre 2020, *op. cit.*, p. 5.

[576] *Idem*, p. 6

[577] CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, p. 5.

[578] *Ibid*.

[579] La proposition de loi n°599 adoptée par l'Assemblée nationale pour une sécurité globale préservant les libertés du 15 avril 2021, *op. cit.*, art. 47 (L. 242-5, I, 1°) prévoyait que pouvait faire l'objet d'un recours à des drones aériens les « crimes ou délits punis d'une peine d'emprisonnement d'une durée supérieure ou égale à cinq ans » tandis que la loi RPSI permet le recours à ces dispositifs par la police judiciaire pour tout « crime ou délit puni d'au moins trois ans d'emprisonnement » (art. 16, CPP art. 230-47, 1°).

du 22 décembre 2020 du Conseil d'État irait d'ailleurs dans ce sens puisque les juges avaient estimé que « le ministre n'apporte pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique ne pourrait être atteint pleinement dans les circonstances actuelles, en l'absence de recours à des drones »[580].

224. À l'instar d'autres systèmes de vidéoprotection, la loi RPSI exige qu'une autorisation soit délivrée préalablement à tout recours à des drones aériens et distingue les autorités compétentes selon qu'il s'agisse d'une activité relevant de la police administrative ou d'une activité de police judiciaire. En reproduisant maladroitement le cadre propre aux caméras fixes, le législateur ne permet pas à cette obligation de constituer une véritable garantie protégeant les droits et libertés dans le cadre du recours à un drone aérien par la police administrative. Le texte prévoit que s'agissant des usages préventifs les autorisations soient délivrées par le préfet territorialement compétent. Cependant, il ressort de l'analyse du professeur Jacques Buisson que compte tenu du fait que les activités de prévention des atteintes à l'ordre public entrent dans le cadre d'une police administrative devenue matérielle et coercitive il aurait été « opportun [de] confier la délivrance [de ces autorisations] à l'autorité de police judiciaire »[581].

225. Aussi, lors de son contrôle des premières dispositions régissant les systèmes de vidéoprotection, le juge constitutionnel avait exigé qu'un contrôle préalable soit effectué par une commission indépendante chargée d'examiner la nécessité et la proportionnalité du recours à des caméras de surveillance filmant la voie publique[582]. De manière similaire, la jurisprudence de la Cour de justice de l'Union européenne (CJUE) formule des exigences en matière de mesures de surveillance, obligeant à ce qu'elles fassent préalablement l'objet « d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect

---

580 CE, 10ème - 9ème chambres réunies, 22 décembre 2020, *op. cit.*

581 BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 14.

582 C. const., Décision 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 6 à 12 ; CSI, art. L. 252-1 : « L'installation d'un système de vidéoprotection dans le cadre du présent titre est subordonnée à une autorisation du représentant de l'État dans le département et, à Paris, du préfet de police donnée, sauf en matière de défense nationale, après avis de la commission départementale de vidéoprotection ».

des conditions et des garanties devant être prévues »[583].

226. Le législateur a pris la décision de confier la responsabilité de ce contrôle *a priori* à la CNIL, qui délivre un avis préalablement à la publication du décret autorisant l'emploi d'un drone aérien de sécurité publique par la police administrative[584]. Néanmoins, il est regrettable qu'aucune condition n'ait été prévue concernant le recours à des drones aériens de sécurité publique dans le cadre d'une procédure d'urgence.

2. Des conditions d'emploi inadaptées aux drones aériens de sécurité publique

227. Les dispositions de la loi RPSI définissent des limites d'emploi des drones aériens de sécurité publique qui se révèlent en pratique inadaptées quant au respect des lieux privés (a) ainsi qu'à la protection des droits des personnes eu égard aux traitements de leurs DACP (b).

a. Des limites spatiales impropres aux drones aériens de sécurité publique

228. Le manque de discernement du législateur à l'égard des particularités des drones aériens de surveillance de la voie publique entache également les dispositions visant à délimiter leur champ spatial d'utilisation par les forces de l'ordre. Ces dispositions sont critiquables à deux égards. D'une part, le professeur Jacques Buisson rappelle que dans le domaine pénal, la notion de lieu clos[585] bénéficie d'une définition plus appropriée puisqu'elle ne se limite pas au seul bâtiment constituant le domicile mais également à « un jardin ou un parc jouxtant un immeuble d'habitation »[586]. En ce sens, cette définition aurait été plus protectrice de la vie privée et notamment du domicile des personnes concernées compte tenu des difficultés particulières que pourront rencontrer les drones aériens pour respecter cette interdiction en comparaison des caméras fixes de vidéoprotection.

---

583 CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, aff. C-511/18, C-512/18 et C-520/18, §§ 139, 168, 179, 189 et 192 [en ligne].

584 CSI, art. L. 242-8.

585 La notion de lieu clos dans le cadre de la police judiciaire a été adoptée par la Cour de cassation (C. cass., ch. crim., 23 mai 1995, n°94-81.141 [en ligne]) et peut être définie comme « celui dans lequel, qu'il soit ou non constitutif de domicile, nul ne peut, en dehors du cadre de la flagrance, pénétrer sans en avoir reçu préalablement l'autorisation de son occupant » (GUINCHARD (S.) et BUISSON (J.), *Procédure pénale*, *op. cit.*, n°614, p. 626). Voir également sur la notion de « lieu clos » : BUISSON (J.), *L'acte de police*, Lyon III, Thèse, 1988, 1237 p., p. 567.

586 BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 14.

D'autre part, il sera difficile de respecter la règle interdisant à tout dispositif de vidéoprotection de filmer l'intérieur des domiciles.

229. La particularité des drones aériens en tant que dispositif de vidéoprotection réside dans leur caractère mobile et leur hauteur de vol. En cela, ces dispositifs diffèrent sensiblement des caméras fixes. Aussi, il semble peu réaliste d'envisager un floutage de l'intérieur de ces lieux privés en temps réel. Il serait toutefois possible - et fortement encouragé - d'envisager que le plan de vol soit préétabli de telle sorte à ce que le drone aérien ne filme que la voie publique. En outre, la rapporteure de la proposition de loi sur la sécurité globale reconnaissait déjà lors des débats en 2020 qu'il « n'est matériellement pas possible d'interdire de visualiser les espaces privés »[587]. Le législateur, conscient de cette difficulté, a donc prévu une « parade » à la captation illégale (certes involontaire) d'images portant sur des lieux privés en laissant le soin aux autorités de les supprimer dans un délai de quarante-huit heures. Toutefois, le législateur instaure une exception à l'effacement de ces images illégalement collectées par des drones aériens lorsqu'elles ont fait l'objet « d'une transmission dans ce délai dans le cadre d'un signalement à l'autorité judiciaire, sur le fondement de l'article 40 du CPP ». Cette exception se révèle alors tout à fait déconcertante puisqu'elle soutient en vérité que des données illégalement collectées pourraient être utilisées lors d'un procès pénal allant pourtant à l'encontre d'un des principes essentiels qui fondent la procédure pénale. Dès lors, le législateur a échoué dans sa tâche de concevoir des dispositions juridiques à la mesure des conséquences que présentent les caractéristiques aérienne et mobile des drones de sécurité publique sur l'exercice des droits et libertés. Il en va autant des droits des personnes au respect du caractère privé de leur domicile que de la protection de leurs DACP.

b. Une protection des DACP insuffisantes à l'emploi de drones aériens de sécurité publique

230. Une obligation d'information imprécise - En conditions réelles, les dispositions issues de la loi RPSI relatives aux caméras aéroportées à l'usage des forces de sécurité publique paraissent fragiles. En ce sens, les garanties prévues en matière d'obligation d'information des personnes concernées de l'emploi de drones aériens de sécurité publique paraissent nettement insuffisantes eu égard à la complexité des conditions de mise en œuvre en pratique. La loi RPSI impose que cette

[587] AN, Débats publics de la troisième séance du vendredi 20 novembre 2020 relatifs à l'amendement n°1164 [en ligne].

information du public pourra se faire par tout moyen, néanmoins il est regrettable qu'aucune précision n'ait été exigée par le Conseil constitutionnel (pas plus que lors de l'examen du texte de la loi sécurité globale). À l'occasion de son contrôle de la première loi introduisant les systèmes de vidéoprotection, le Conseil avait imposé aux autorités publiques de s'assurer « que le public soit informé de manière claire et permanente de l'existence du système de vidéosurveillance ou de l'autorité et de la personne responsable »[588] avant d'autoriser le recours à ces dispositifs. En outre, la DPJ impose au responsable de la mesure de surveillance de délivrer plusieurs informations aux personnes concernées s'agissant de la collecte de leurs données, telles que l'identité du responsable de traitement, les finalités du traitement ou encore les droits qu'elles peuvent exercer[589].

231. En pratique, il s'avère difficile d'imaginer comment cette obligation sera mise en œuvre compte tenu de la miniaturisation et de la hauteur de vol de ces drones aériens qui même lorsqu'ils sont équipés de signaux visuels ou sonores peuvent encore échapper à l'attention des personnes observées. En outre, la seule information de leur emploi au public est insuffisante puisque leur caractère mobile ne permet pas aux personnes d'être averties de manière continue de leur présence. Ces dispositions relatives à l'obligation d'information des personnes sont d'autant plus inquiétantes qu'elles comprennent de nombreuses exceptions déjà relevées par la CNIL en 2021, qui recommandait par conséquent que celles-ci soient précisées par un texte réglementaire[590]. Elle réitèrera son inquiétude quant aux limites portées au droit à l'information des personnes concernées[591] lors de l'examen du projet de décret précisant le cadre d'emploi des caméras aéroportées estimant que cette exception était trop étendue[592]. Afin de faciliter la mise en œuvre concrète de l'obligation d'information du recours à cette technologie par les forces de l'ordre, la CNIL recommandait que celle-ci soit délivrée sur le lieu de l'opération prévue et suggérait d'avoir

---

[588] C. const., Décision 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 5.

[589] DPJ, art. 13.

[590] CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, p. 7.

[591] CSI, art. R. 242-13.-I. : « L'information du public sur l'emploi des caméras installées sur des aéronefs est délivrée par tout moyen approprié, sauf si l'urgence ou les conditions de l'opération l'interdisent ou si cette information entre en contradiction avec les objectifs poursuivis ».

[592] CNIL, Délibération n° 2023-027 du 16 mars 2023, *op. cit.* : « la rédaction " sauf si les circonstances l'interdisent " telle que mentionnée au I de l'article R. 242-6 du CSI est particulièrement large et, par conséquent, accueille favorablement les modifications réalisées ».

recours à des dispositifs sonores[593] notamment lors de leur utilisation à des fins d'encadrement des manifestations[594]. Une fois encore les recommandations de la CNIL n'ont malheureusement pas été prises en considération, le décret n'apportant pas davantage de précisions[595].

232. Un traitement de DACP disproportionné et imprécis - Face aux enjeux que présentent les drones aériens de sécurité publique pour les droits et les libertés, le législateur a tenu à limiter le traitement de DACP en renforçant le principe de minimisation, qui exige que seules les données strictement nécessaires aux finalités pourront être collectées[596]. Toutefois, cette garantie ne peut être effective que dans le cas où les dispositifs mis en œuvre ont été conçus dans le respect des règles relatives à la protection des DACP dès la conception et par défaut[597]. Partant du constat que les forces de l'ordre ont eu recours à des drones aériens préalablement à toute législation spécifique et que le ministère de l'Intérieur a été sanctionné pour défaut de déclaration à la CNIL de ces usages, il serait recommandé de s'assurer que les dispositifs utilisés respectent effectivement ces règles. En outre, l'enjeu central des drones aériens de sécurité publique repose sur le type de données qu'ils collectent.

233. Certaines DACP collectées peuvent entrer dans la catégorie des données reconnues comme « sensibles » par la règlementation relative à la protection des DACP[598], telles que les données biométriques ou des données relatives aux opinions politiques, à l'appartenance syndicale ou aux convictions religieuses (notamment lors de la surveillance de manifestations sur la voie publique). En outre, les drones aériens de sécurité publique pourraient analyser des données telles que la démarche à des fins de suivi d'une personne sur la voie publique, données qui sont reconnues

---

[593] Le message sonore pourrait délivrer les informations concernant notamment les finalités ou encore le nom de l'entité responsable du traitement des données, à l'image des panonceaux informant de l'usage d'une caméra fixe de vidéoprotection (voir la fiche récapitulative de la CNIL relative à la vidéoprotection sur la voie publique [en ligne]). Il convient de noter que s'agissant des caméras individuelles portées par les agents l'information aux personnes est délivrée au moment de l'enregistrement des images (CSI, art. L. 241-1 : « Le déclenchement de l'enregistrement fait l'objet d'une information des personnes filmées ») et qu'il n'en va pas de même pour les caméras aéroportées.

[594] CNIL, « L'usage des drones par les forces de l'ordre », 27 avril 2023 [en ligne].

[595] Décret n° 2023-283 du 19 avril 2023 relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs pour des missions de police administrative, *op. cit.*, art. R. 242-13.-I.

[596] CSI, art. L. 242-4, al. 1er.

[597] DPJ, art. 20.

[598] DPJ, art. 10 et LIL, art. 6 §1.

par la CNIL comme étant des DACP biométriques[599]. En ce sens, des études sur le mouvement humain démontrent que la démarche d'une personne permet de l'identifier comme une seule et même personne[600]. Il convient de noter que la CNIL est une des rares autorités de protection des DACP à attribuer aux données relatives à la démarche le caractère de données biométriques. Ce constat est loin d'être anodin dans la mesure où toute donnée qualifiée de sensible fait précisément l'objet d'une procédure de traitement plus stricte[601] - y compris s'agissant des forces de l'ordre[602]. La CNIL démontre là encore qu'elle se montre particulièrement vigilante vis-à-vis des DACP collectées et plus particulièrement s'agissant des forces de l'ordre dont les mesures de police consistent précisément à restreindre l'exercice des droits et libertés afin de répondre aux besoins de l'ordre public.

234. Aux fins de protéger les données dites sensibles, la règlementation protégeant les DACP exige une démonstration préalable par les autorités publiques de la « nécessité absolue » de collecter ce type de données[603] afin de ne pas porter une atteinte disproportionnée au droit à la vie privée et à la protection des données. En d'autres termes, les forces de l'ordre doivent être en mesure de démontrer qu'elles ne disposent pas d'alternatives moins invasives à des fins de sauvegarde de l'ordre public que d'avoir recours à des drones aériens collectant ce type de données. Compte tenu du fait que le préfet territorialement compétent sera le seul juge du caractère nécessaire et proportionné de l'utilisation des drones aériens à des fins de police administrative il faut espérer qu'il se montrera particulièrement exigeant pour justifier de leur usage et des données pouvant être collectées. Il ne faudrait pas que la simple rapidité d'exécution des missions ou l'avantage économique puisse suffire à justifier de la nécessité d'avoir recours à un tel dispositif de surveillance. En ce sens, la CNIL encourageait les autorités à évaluer l'efficacité du recours à des

---

599 Voir notamment : CNIL, Définition « Biométrie », *cnil.fr* [en ligne] ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

600 « Des études récentes suggèrent que le patron de marche peut permettre d'identifier les individus. Si un algorithme est en mesure de classifier (reconnaître) les individus, cela signifie que chaque individu possède son propre patron de marche, et donc une signature individuelle » (issu du MOOC sur « Le mouvement humain » élaboré par le Laboratoire des Sciences et techniques des activités physiques et sportives de l'Université de Nantes, disponible en ligne sur la plateforme FUN). Voir principalement : HORST (F.) *et al.*, "Explaining the unique nature of individual gait patterns with deep learning", *Sci Rep.*, February 20th 2019, 2391. Voir aussi : AELES (J.) *et al.*, "Revealing the unique features of each individual's muscle activation signatures", *J R Soc Interface*, January 18th 2021 ; HUG (F.) *et al.*, "Individuals have unique muscle activation signatures as revealed during gait and pedaling", *J Appl Physiol* (1985), October 1st 2019, 127(4), pp.1165-1174.

601 RGPD, art. 9 ; LIL, art. 6.

602 DPJ, art. 10 ; LIL, art. 88.

603 LIL, art. 6 §3, 31 et 32 ;

drones aériens et rappelait l'intérêt de l'étude d'impact imposée aux autorités préalablement à toute collecte de DACP[604].

235. En dépit des conditions exigées et de la réserve d'interprétation formulée par le Conseil constitutionnel s'agissant des traitements automatisés de DACP, celles-ci ne prennent pas suffisamment en compte toutes les potentialités d'atteintes aux droits et libertés que présentent les drones aériens de sécurité publique. Le fait est que l'interdiction du recours à des traitements automatisés de reconnaissance faciale de manière directe ou indirecte par l'intermédiaire d'un drone aérien de sécurité publique n'ôte en rien l'effet d'amplification de la surveillance. La controverse à laquelle font face les systèmes de reconnaissance faciale n'est que le fruit des résultats parfois désastreux engendrés par cette technologie, tant dans le cadre d'une utilisation à des fins commerciales qu'à des fins policières[605]. Les débats se sont ainsi largement étendus sur ce sujet sans pour autant prendre en considération les autres effets que peuvent avoir le traitement d'autres données (biométriques ou non) ou le recours à d'autres algorithmes d'analyse d'événements. Le fait est que les données servant au processus décisionnel des algorithmes à l'usage des forces de l'ordre ne se limitent pas aux seuls traits du visage permettant une reconnaissance faciale.

236. Enfin, il peut être reproché au Conseil constitutionnel de n'avoir pris en considération que le droit à la protection de la vie privée dans le cadre de son examen des dispositions relatives à l'usage des drones aériens de la loi RPSI. Pourtant, les recours croissants aux technologies de surveillance par les forces de l'ordre ont une incidence sur de nombreux autres droits et libertés[606]. En matière de vidéoprotection, les droits et libertés pouvant faire l'objet d'une limitation ne manquent pas. La liberté d'aller et venir apparait naturellement comme la première liberté dont l'exercice est limité par la vidéoprotection. En l'occurrence, il s'agit plus précisément d'une des conditions inhérentes à cette liberté permettant à quiconque de pouvoir circuler librement sur la voie publique de manière anonyme. Il est dès lors surprenant que les Sages se soient limités au droit à la

---

[604] CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, p. 4.

[605] De manière non-exhaustive : Sénat, Rapport d'information fait au nom de la commission des lois n° 627 (2021-2022) remis par DAUBRESSE (M-P.), de BELENET (A.) et DURAIN (J.) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », 10 mai 2022, pp. 32-34 [en ligne] ; CNIL, « Reconnaissance faciale - Pour un débat à la hauteur des enjeux », *op. cit.* ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, pp. 73-74 ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.* pp. 50-51.

[606] CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*, p. 4.

vie privée[607] alors que les drones aériens exercent une pression nettement plus élevée sur la liberté d'aller et venir puisqu'ils sont en mesure d'effectuer le suivi d'un individu lors de ses déplacements sur la voie publique voire de l'identifier[608]. À ce sujet, la CNIL avait déjà souligné l'importance de ce droit à l'anonymat et à la liberté de pouvoir se déplacer sans être surveillé[609].

237. Le droit de manifester pourrait également être nettement restreint par ces usages puisque la loi prévoit la possibilité d'avoir recours à des drones aériens à des fins de surveillance des manifestations sur la voie publique. En dépit de sa légitimité, cette finalité porte atteinte au droit de manifester. En ce sens, la présence des drones aériens pourrait engendrer un effet dissuasif des participants sans distinction. De fait, leurs caractères discret et omniscient sont susceptibles de susciter la crainte d'une surveillance dissimulée et ainsi de conditionner le comportement des personnes observées. En outre, le texte se présente comme moins protecteur des droits et libertés que ne l'était la version de la loi de 2021, qui exigeait que le recours à ces dispositifs à des fins de surveillance des rassemblements sur la voie publique soit conditionné par un risque de troubles « d'une particulière gravité » à l'ordre public[610].

238. L'absence de clairvoyance du Conseil constitutionnel quant aux autres usages technologiques qui pourraient être associés aux drones aériens de sécurité publique est ce qui a permis aux autorités publiques d'envisager le recours à des algorithmes d'analyse d'images[611]

---

607 La proximité entre la condition d'anonymat des déplacements issue de la liberté d'aller et venir, d'une part, et, le droit à la vie privée d'autre part pourrait-elle expliquer les raisons pour lesquelles le Conseil constitutionnel ne s'est reposé que sur le droit à la vie privée pour examiner la constitutionnalité de la loi RPSI ? Cette explication viendrait cependant remettre en question la jurisprudence actuelle du juge constitutionnel qui reconnait ces deux libertés comme indépendantes l'une de l'autre tout en étant des composantes de la liberté personnelle.

608 C'était ce qu'avait notamment souligné la CNIL lors de sa délibération n° 2021-011 du 26 janvier 2021, *op. cit.*, pp. 4-6.

609 *Idem* ; CNIL, 24ème Rapport d'activité de 2003, *La Documentation française*, 2004, p. 135 [en ligne].

610 En ce sens, le Conseil des droits de l'homme de l'ONU avait déjà souligné lors de la loi de 2021 une dangereuse augmentation des limites posées aux droits et libertés par le recours à ces dispositifs notamment par la surveillance étendue des manifestants au nom de la sécurité et de la lutte contre le terrorisme. Les membres de l'ONU craignaient ainsi que ces usages puissent avoir de graves répercussions sur les droits et libertés en France mais aussi dans d'autres pays qui souhaiteraient mettre en œuvre une législation similaire (ONU - Conseil des droits de l'homme, Commentaires et suggestions à propos de la proposition de loi n° 3452 relative à la sécurité globale datant du 20 octobre 2020, 12 novembre 2020 [en ligne]).

611 Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 99 : « Il pourrait être envisagé, à titre d'exception, d'autoriser l'utilisation de la reconnaissance biométrique sur la voie publique en temps réel dès lors que celle-ci serait strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes, en cas de menace grave et imminente pour la sécurité nationale ou dans le cadre d'une enquête judiciaire pour une infraction suffisamment grave ».

notamment à titre expérimental pour les grands évènements prévus en France en 2023 et 2024[612]. Pour faire face à l'augmentation exponentielle des images issues des caméras (fixes comme mobiles) au sein de l'espace public, les autorités envisagent d'utiliser des technologies d'IA afin d'analyser et d'interpréter en temps réel l'importante quantité d'images qu'un être humain ne serait pas en mesure d'effectuer. Cependant, ces technologies ne disposent encore d'aucune législation nationale ou européenne permettant d'encadrer leurs usages de manière spécifique.

Section 2 La nécessité d'un cadre juridique *ad hoc* des caméras aéroportées « augmentées » de sécurité publique

239. Les algorithmes ont intégré de nombreuses activités de la vie quotidienne et peuvent s'adapter à de multiples domaines[613], y compris les domaines régaliens tels que la police ou la justice. Il convient de mentionner à ce propos que les algorithmes employés dans le domaine régalien ne reposent pas tous sur un traitement massif de données ou sur un apprentissage machine mais qu'en revanche « ils incluent tous un traitement automatique de données en vue de parvenir à une décision qui peut avoir des conséquences importantes, positives ou négatives, pour les personnes concernées »[614].

240. Les algorithmes « augmentés » à l'usage de la sécurité publique font progressivement leur entrée dans l'arsenal des forces de l'ordre en France, quand d'autres pays en font déjà un usage fréquent[615]. Toutefois, les finalités de recours à ces algorithmes peuvent être distinctes selon les pays, les rendant plus ou moins intrusifs et présentant des conséquences plus ou moins graves pour

---

612 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 5 : « La détection automatisée d'anomalies dans l'espace public (ex. mouvements de foule, bagarres) ainsi que le renforcement d'accès à des sites sensibles […] pourraient être autorisés par voie législative, à des fins de tests. Leur utilité serait particulièrement marquée dans la préparation des grands événements de 2023 et 2024, ce qui nécessite à court terme de mener des expérimentations afin de vérifier les apports opérationnels réels, les conditions de déploiement et le cadre d'emploi ».

613 De manière non-exhaustive : DELTORN (J-M) et PICHENOT (E.), « Introduction - Entre risques et opportunités : de l'usage des algorithmes », *in* DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.*, pp. 5-6 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 13 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 93 ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 7.

614 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 17.

615 Centre des Hautes Études du Ministère de l'Intérieur (CHEMI), Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), 12 juillet 2019, 86 p. [en ligne] ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, spéc. pp. 73-76.

les personnes[616]. S'agissant des caméras « augmentées » filmant la voie publique, divers usages ont pu être observés. Aussi, les recherches dans ce domaine présentent d'autres potentialités d'utilisation, même si certaines resteront au stade purement exploratoire (§1). Aussi, les différents usages et expérimentations des caméras « augmentées » de sécurité publique nécessitent un encadrement juridique permettant d'assurer la protection des droits et libertés auxquels cette technologie pourrait porter atteinte. Or, la réglementation applicable aux technologies reposant sur des algorithmes demeure peu étendue, y compris s'agissant du domaine régalien, et se limite généralement à celle afférente à la protection des DACP (§2).

§1. Les caméras « augmentées » de sécurité publique : usages et perspectives

241. Ces dernières années, les autorités publiques ont exploré la possibilité d'intégrer des technologies d'IA au cœur de leurs activités en vue d'améliorer la sécurité des personnes et des biens[617]. Parmi les différentes applications qui ont été progressivement intégrées ou pourraient être prochainement intégrées se trouvent les technologies d'IA reposant sur des systèmes algorithmiques d'aide à la décision (SAAD) à des fins d'analyse d'images issues de caméras de vidéoprotection[618]. Les algorithmes associés aux caméras de vidéoprotection peuvent être intégrés soit dans les systèmes d'information du centre de commandement qui reçoivent les données en temps réel, soit directement dans le système de vidéoprotection. Ces caméras enrichies d'algorithmes ne se limitent alors plus à la simple collecte d'images mais sont en mesure d'effectuer une première analyse des évènements à partir des données collectées.

---

[616] CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, pp. 13-14.

[617] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.* ; Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, spéc. pp. 150-152 et pp. 219-225 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.* ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.* ;

[618] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, spéc. pp. 30-31 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.* ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.* ;

242. Aujourd'hui, les systèmes de vidéoprotection sont souvent associés à des algorithmes d'analyse d'images[619]. Ces dispositifs, désignés sous les termes de caméras « augmentées » ou de caméras « intelligentes », sont composés « de logiciels de traitement automatisés d'images associés à des caméras, permettant d'extraire diverses informations à partir de flux vidéo qui en sont issus »[620]. Outre les informations qu'ils fournissent, ces logiciels présentent « un réel intérêt pour les centres de supervision qui emploient des opérateurs nombreux visionnant de plus en plus de caméras »[621] et leur assurent un traitement en temps réel des évènements. Ces technologies sont désormais en mesure de détecter des individus en mouvement ou des objets abandonnés et d'alerter un opérateur de toute anomalie mais pourraient prochainement intégrer une analyse en temps réel du comportement humain en s'appuyant sur des données biométriques ou comportementales[622].

243. Les différentes finalités des caméras « augmentées » - Les caméras « augmentées » peuvent viser différents objectifs. Il est ainsi possible de classer les systèmes d'aide algorithmiques au traitement d'images selon quatre niveaux[623]. Le premier niveau repose sur la détection de la présence d'objets ou d'individus dans une image ou une vidéo sans en déterminer la nature. Le deuxième niveau permet une première analyse des évènements par une reconnaissance et une catégorisation des éléments en présence[624]. Le troisième niveau permet d'identifier un objet ou un individu à partir de données non biométriques sans réidentification. Dans le cas d'une personne, les systèmes algorithmiques de traitement d'images de troisième niveau effectuent une

---

619 Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 12 et 85 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 3.

620 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 3.

621 MELCHIOR, Philippe, « Vidéoprotection : sert-elle à quelque chose ? », p. 105 *in* DOUILLET, Anne-Cécile, GERMAIN, Séverine, HELLEMAN, Éric, et MELCHIOR, Philippe, *Vidéo-surveillance ou vidéo-protection ?*, *op. cit.*

622 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 6 et 9 ; STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *American Civil Liberties Union* (ACLU), June 17th 2019, pp. 20-22 [en ligne] consulté le 7 mars 2023.

623 Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 26.

624 À titre d'exemple, ces algorithmes peuvent effectuer une analyse des mouvements anormaux de foule, déterminer le parcours suivi par un ou plusieurs individus au sein de l'espace public ou d'établissements privés ouverts au public, effectuer un comptage de personnes, détecter des comportements suspects, etc.

individualisation[625] ; en d'autres termes ils isolent la personne d'autres éléments ou personnes afin d'effectuer son suivi sans lui attacher d'identité[626]. Enfin, le quatrième niveau de système algorithmique d'analyse d'images consiste à reconnaitre, et donc à identifier, un individu à l'aide de ses données biométriques (ex. visage, iris, démarche, etc.). Par conséquent, les algorithmes d'analyse d'images peuvent procéder à l'identification de personnes à partir de différents types de données à caractère personnel (sensibles ou non) ou non personnel (ex. vêtements ou objets portés).

244. L'introduction de ces algorithmes constitue une extension des pouvoirs de l'État où les outils iront au-delà de la simple prévention des atteintes à l'ordre public pour chercher à anticiper les évènements à l'aide d'algorithmes « augmentés »[627]. Ainsi, plus qu'à identifier une personne, les autorités de sauvegarde de l'ordre public s'intéressent aux outils leur permettant de prévenir les évènements. Certains auteurs évoquent alors les termes de « police prédictive »[628]. L'emploi du terme « prédictif » est critiquable à deux égards. D'une part, la notion de « police prédictive » repose sur une traduction erronée des systèmes prédictifs utilisés aux États-Unis désignés par les termes de *predictive policing*[629]. Ainsi, la « police prédictive » ne repose pas sur le fait « de prédire la police mais plutôt d'appliquer des méthodes d'analyse prédictive qui vont permettre aux services de police et de gendarmerie d'empêcher la criminalité »[630]. D'autre part, il convient d'employer prudemment le terme « prédictif » car la notion de « prédiction » sous-entend une vision certaine du

---

[625] Or, l'individualisation constitue un traitement de DACP au sens de la CNIL et du CEPD (CNIL, « Identifier les données personnelles », 27 janvier 2020 [en ligne] : Pour qu'un jeu de données soit considéré comme anonyme (et donc sorte du cadre de la protection des DACP), il « doit nécessairement résulter d'un processus d'anonymisation qui éliminera toute possibilité de ré-identification des individus [tel que] l'individualisation [où] il n'est pas possible d'isoler une partie ou la totalité des enregistrements relatifs à un individu » ; G29, Avis 05/2014 sur les Techniques d'anonymisation, 10 avril 2014, 42 p., p. 13 [en ligne] : « L'individualisation correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données »).

[626] À titre d'exemple, ils peuvent effectuer le suivi d'un individu dans une foule à l'aide des vêtements portés, des objets transportés ou encore des tatouages, etc.

[627] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 74.

[628] Voir notamment : Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 150-152 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, spéc. pp. 93-111.

[629] Bien que le terme anglais « *predictive »* puisse effectivement signifier « prédictive » en français, il n'en va pas de même pour le terme « *policing* » qui évoque la notion de contrôle ou de surveillance et non pas de « police ».

[630] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 67.

futur qui pourtant ne l'est pas[631]. Dès lors, il est préférable de désigner ces SAAD sous les termes d'outils d' « analyse décisionnelle »[632].

245. En France, l'usage de ce type d'algorithmes « augmentés » à des fins de sécurité publique diffère des usages pratiqués à l'étranger dans la mesure où ils ne se destinent pas véritablement à la protection des personnes mais plutôt à assurer la protection de leurs biens[633]. Dans d'autres cas, leur utilisation repose davantage sur des scénarios fictifs ou un développement expérimental. Les outils de police « augmentée » se fondent sur des algorithmes d'IA dont l'objectif consiste à anticiper des événements par une agrégation des données historiques à de nouvelles informations[634]. En d'autres termes, l'algorithme fonctionne à partir des données issues de son apprentissage, agrégées à celles collectées en cours de mission.

246. Il existe une grande diversités d'outils algorithmiques à l'usage des activités de police et de secours, dont certains peuvent ou pourraient être utilisés à des fins d'analyse d'images issues de caméras de vidéoprotection (A). Aujourd'hui, ces algorithmes « augmentés » sont susceptibles d'être associés aux dispositifs de surveillance de la voie publique, principalement à des fins d'encadrement de grands évènements[635]. Une projection de l'utilisation de ces outils semble alors pertinente et nécessaire afin d'évaluer leurs conséquences sur les droits et libertés (B).

---

631 Dans le même sens, Aurélie Jean préfère l'emploi du terme « algorithmisé » qui « exprime plus précisément ce qui est fait, à savoir algorithmiser certaines parties [d'un domaine] afin d'obtenir des éléments de prédiction et d'analyse […] et non de prédire *stricto sensu* » (JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 15).

632 CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, pp. 8-9 ; Gendarmerie nationale, « La Gendarmerie, de l'analyse prédictive à l'analyse décisionnelle », *L'essor de la gendarmerie nationale*, 26 janvier 2018 [en ligne].

633 INHESJ, « Anticiper le crime : généalogie, actualité et perspectives », 25 février 2020 [en ligne] : en effectuant une analyse statistique des zones faisant le plus fréquemment l'objet de vols (habitations ou voitures).

634 CASTETS-RENARD (C.), « L'IA en pratique : la police prédictive aux États-Unis », *Dalloz IP/IT*, n°5, 15 mai 2019, p.314.

635 À ce sujet, le Livre blanc de la sécurité intérieure en constitue un bon exemple (Ministère de l'Intérieur, *Livre blanc de la sécurité intérieure*, *op. cit.*). Voir aussi : Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, pp. 150-151 ; Sénat, Rapport d'information fait au nom de la commission des lois n° 627 (2021-2022) remis par DAUBRESSE (M-P.), de BELENET (A.) et DURAIN (J.) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*

A. Les algorithmes « augmentés » à des fins de sécurité publique : les potentialités des caméras « augmentées » de sécurité publique

247. Il existe une multiplicité d'usages des caméras lorsqu'elles sont accompagnées d'outils algorithmiques d'IA permettant une analyse en temps réel (ou différé) des évènements qu'elles entrent dans un cadre de police administrative ou de police judiciaire. Les usages de cette technologie peuvent s'avérer plus ou moins intrusifs selon le type de données collectées. L'objectif de ces caméras « augmentées » peut être d'avoir une vue d'ensemble des évènements, comme le fait d'observer une foule sans pour autant cibler les personnes, dont la finalité est moins intrusive que celle de suivre un individu en particulier.

248. Une des premières formes d'utilisation d'outils algorithmiques d'analyse d'images à des fins de sécurité publique porte sur les systèmes de détection et de sanction automatisées des excès de vitesse[636]. Les images vidéo sont analysées afin d'en extraire les numéros d'immatriculation des véhicules ayant dépassé la limite autorisée et d'identifier les potentiels auteurs de l'infraction ou de tout acte criminel[637]. Des dispositifs similaires en matière de sécurité routière ont progressivement fait leur apparition au sein de l'espace public, tels que les caméras de détection de non-respect d'un sens interdit ou d'un feu rouge.

249. Aujourd'hui, de nombreux types d'outils algorithmiques équipant les caméras de vidéoprotection peuvent servir à analyser des personnes de manière individuelle (ciblage) ou groupé (foule) à des fins d'identification (ex. reconnaissance faciale[638]) ou non (ex. détection de présence d'un être humain). Jay Stanley, auteur d'une étude pour l'*American Civil Liberties Union* (*ACLU*) portant sur les caméras de surveillance dotées d'algorithmes d'IA[639], répertorie différentes formes d'application d'algorithmes d'IA à des caméras de surveillance dont certaines peuvent ou pourraient s'appliquer au cadre de la sécurité publique.

---

[636] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 30.

[637] CSI, art. L.233-1 à L. 233-2.

[638] Note : l'usage d'outils de reconnaissance faciale étant interdite dans le cadre de l'utilisation de caméras aéroportées cette technologie ne fera pas l'objet d'une analyse approfondie dans le cadre de cette étude.

[639] STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit*.

250. L'utilisation d'outils algorithmiques d'analyse d'images de vidéoprotection peut permettre la détection de la présence d'individus ou d'objets mais aussi des actions d'un ou de plusieurs individus (*activity and action recognition*). Cette technique se décline en plusieurs sous finalités telles que la détection de présence permettant le déclenchement d'une alarme d'intrusion dans une zone interdite d'accès. Ce type de technique de sécurité n'est pas nouvelle en soi mais ici l'algorithme d'IA permet de « tracer » une zone en la délimitant par des « lignes » virtuelles[640]. Cette technique pourrait être utilisée pour contrer les intrusions de sites tels que des immeubles en construction, des zones dangereuses (ex. risque d'éboulement) ou encore une centrale nucléaire (ex. notamment pour contrer les survols illégaux de site par des drones aériens civils).

251. Une autre forme d'utilisation d'algorithme d'analyse d'images consiste à détecter et à envoyer une alerte lorsqu'un individu se déplace dans le sens inverse du mouvement général d'une foule. L'algorithme cible une zone précise et enverra une alerte lorsqu'une personne ira dans la « mauvaise direction »[641]. Sur un principe similaire, certains algorithmes d'analyse d'images permettent la détection de personnes en train de courir (hors contexte « sportif »)[642]. Enfin, l'analyse d'images permettant la détection d'individus allongés au sol ou inanimés[643] peut s'avérer intéressante, notamment pour les services de secours.

252. Aujourd'hui, les recherches en la matière permettent de détecter des actions de plus en plus complexes[644] impliquant de nombreuses personnes ou objets, offrant de réelles perspectives d'améliorations de détection d'actes suspects. La détection de présence et d'actions par analyse

---

640 Voir notamment : IntelliVision - Real-time AI Video Analytics Processing [en ligne] consulté le 3 avril 2023.

641 Voir notamment : AXIS Camera Application Platform (ACAP) - AXIS Direction Detector [en ligne] consulté le 3 avril 2023.

642 Il s'agit de détecter le moment où une ou plusieurs personnes commencent à courir (pouvant signaler la présence d'un danger) ou lorsqu'elle(s) s'arrête(nt), voire même de détecter une variation anormale de la vitesse ou de l'accélération d'un individu. Voir notamment : Honeywell - Système vidéo d'analyse de scènes [en ligne] ; PARIPALLY (G.) and CONTROLS (J.), "Artificial Intelligence Will Revolutionize Physical Security: Intelligent, Autonomous Systems That Prevent Incidents Are Coming", 9th November 2021 [en ligne] consultés le 3 avril 2023.

643 Cette fonction était attendue dans le cadre des développements de drones aériens du projet FUI COOPOL afin de détecter des personnes en détresse dans un bâtiment sujet à un incendie à l'aide de caméras thermiques offrant une visibilité à travers la fumée.
Voir notamment : IBM - Lying body detection, 3 mars 2021 [en ligne].

644 STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit.*, p. 14 ; RYOO (M. S.), "Human Activity Prediction : Early Recognition of Ongoing Activities from Streaming Videos", *2011 International Conference on Computer Vision*, Barcelona, Spain, 2011, pp. 1036-1043 [en ligne] ; BARADEL (F.), WOLF (C.), MILLE (J.) and TAYLOR (G. W.), "Glimpse Clouds: Human Activity Recognition from Unstructured Feature Points", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 469-478 [en ligne].

d'images n'entre pas dans la catégorie des techniques les plus intrusives car elle ne repose pas sur une finalité d'analyse de DACP[645]. Ces techniques peuvent toutefois isoler un individu au sein d'une foule qui irait à contre-sens du mouvement menant éventuellement à une individualisation de celui-ci. Dès lors, les données collectées ne seraient plus anonymes et entreraient dans le cadre de la protection des DACP nécessitant notamment l'adoption d'un texte législatif ou réglementaire après avis motivé de la CNIL (s'agissant des forces de l'ordre) ainsi qu'une mention d'information du traitement de DACP aux personnes concernées[646].

253. Une autre technique, plus intrusive cette fois, repose sur la détection d'anomalies car elle consiste notamment à détecter le comportement des individus surveillés. La détection d'anomalies par les systèmes de surveillance automatisés repose sur une association de techniques de détection automatique à des techniques de suivi d'objets ou d'individus « suspects »[647]. Certains systèmes de caméras comportent un programme ayant pour finalité la détection de certains comportements prédéfinis comme « anormaux »[648]. D'autres systèmes de caméras disposent d'un programme plus avancé où l'algorithme augmenté d'une caméra apprend de manière autonome ce qu'est une situation ou un comportement normal(e)[649].

254. Aussi, les recherches dans le domaine des caméras « augmentées » se dirigent progressivement vers une étude contextuelle qui traite des éléments ou informations pouvant fournir un contexte nécessaire à une analyse plus approfondie dans la détection d'activités considérées

---

645 Les DACP peuvent faire l'objet d'un traitement mais sont anonymisées à bref délai. L'algorithme se contente d'analyser la forme du gabarit pour déterminer s'il s'agit d'un être humain ou d'un objet (et éventuellement de quel type d'objet il peut s'agir). Les finalités ne reposent pas sur une identification de personnes.

646 LIL, art. 48, 89 I° et 104 ; RGPD, art. 12 et 14 ; DPJ, art. 13 ; CSI, art. L. 242-8 et L. 255-1.

647 HE (K.), ZHNG (X.), REN (S.) and SUN (S.), "Deep Residual Learning for Image Recognition", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770-778 [en ligne].

648 KE (S.) *et al.*, "A Review on Video-Based Human Activity Recognition", *Computers*, vol. 2, June 5th 2013, pp. 88–131 [en ligne] ; BERMEJO (E.), DENIZ (O.), BUENO (G.) and SUKTHANKAR (R.), "Violence Detection in Video Using Computer Vision Techniques", *International Conference on Computer Analysis of Images and Patterns* (CAIP) 2011, pp. 332-339 [en ligne] ; HASSNER (T.), ITCHER (Y.) and KLIPPER-GROSS (O.), "Violent Flows: Real-Time Detection of Violent Crowd Behavior", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2012, pp. 1-6 [en ligne] ; CHEN (D.) *et al.*, "Recognition of Aggressive Human Behavior Using Binary Local Motion Descriptors", *Annual International Conference IEEE Eng Med Biol Soc.* 2008 [en ligne].

649 Dans cette deuxième forme d'apprentissage, un très grand volume de données vidéo de situations « normales » d'une scène en particulier est utilisé afin d'entrainer l'algorithme d'IA. Il doit ensuite effectuer de nouvelles observations à partir de ses données d'apprentissage pour déterminer par lui-même si la situation observée est « anormale ou inhabituelle par rapport au modèle d'entrainement ». Voir pour exemple : KE (S.) *et al.*, "A Review on Video-Based Human Activity Recognition", *op. cit.*

comme suspectes[650]. Ces données de contexte peuvent notamment porter sur des indices visuels. Les indices visuels peuvent reposer sur des informations démographiques (âge[651], genre, origine ethnique, etc.)[652], les aspects physiques (ex. couleur de peau[653], personne chauve, etc.), les vêtements et l'apparence physique (ex. type et couleur des vêtements), la détection d'objets[654] (objet transporté par un individu), la gestuelle[655] ou l'expression faciale[656] d'un individu (ex. action de la main, reconnaissance d'émotions, etc.), la démarche d'une personne[657], ou encore la reconnaissance de tatouages[658].

255. Les capacités d'analyse de ce type de données pourraient se révéler particulièrement utiles dans le cadre d'une surveillance de grands rassemblements. L'analyse contextuelle d'images peut ainsi s'avérer plus ou moins intrusive selon les usages (en fonction du type de données et

---

650 À titre d'exemple, il s'agirait de prêter plus attention au type de vêtements portés par une personne en fonction du contexte (ex. environnement, météorologie, etc.).

651 ZENGWEI (H.) *et al.*, "Deep Age Distribution Learning for Apparent Age Estimation", *IEEE Conference on Computer Vision and Pattern Recognition* (CVPR), 2016 [en ligne].

652 CHEONG (K.H.) *et al.*, "Practical Automated Video Analytics for Crowd Monitoring and Counting", *IEEE*, vol. 7, January 2019 [en ligne].

653 VINCENT (J.), "IBM secretly used New York's CCTV cameras to train its surveillance software", *The Verge*, September 6th 2018 [en ligne] ; JOSEPH (G.) and LIPP (K.), "IBM used NYPD surveillance footage to develop technology that lets Police Search by Skin Color", *The Intercept_*, September 6th 2018 [en ligne].

654 KITANI (K.M.), ZIEBART (B.D.), BAGNELL (J.A.) and HEBERT (M.), "Activity Forecasting", *Computer Vision – ECCV* 2012 [en ligne].

655 DE SMEDT (Q.), WANNOUS (H.), VANDEBORRE (J-P.), "Skeleton-based Dynamic hand gesture recognition", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2016, pp. 1206-1214 [en ligne].

656 Il ne s'agit pas de reconnaissance faciale dans le sens où la finalité n'est pas d'identifier un individu par ses données biométriques mais d'identifier des expressions du visage communes aux êtres humains afin d'anticiper les potentiels agissements d'une personne.

657 Comme souligné précédemment ce type de données est à caractère unique et permet donc d'identifier directement une personne. Voir notamment : KE (S.) *et al.*, "A Review on Video-Based Human Activity Recognition", *op. cit.* L'analyse de la démarche d'un individu peut également révéler des informations sur une potentiel blessure ou sa condition physique (ex. handicap). Voir à ce sujet : SANCHEZ-DELACRUZ (E.) *et al.*, "Gait Recognition in the Classification of Neurodegenerative Diseases", *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services. UCAmI 2014*, December 2014, pp. 128-135 [en ligne].

658 Le FBI et le NIST américains ont constitué une base de données regroupant 100 000 tatouages (voir notamment : NGAN (M.) and GROTHER (P.), "Tattoo recognition technology - challenge (Tatt-C): an open tattoo database for developing tattoo recognition research", *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, 2015, pp. 1-6 [en ligne] ; NIST, "Tattoo Recognition Technology", July 13th 2017 [en ligne] ; MACKEY (A.) and MAAS (D.), "Tattoo Recognition Research Threatens Free Speech and Privacy", *Electronic Frontier Foundation* (EFF), June 2nd 2016 [en ligne] consulté le 13 avril 2023). Il est aisément envisageable de constituer une telle base de données sans même obtenir le consentement des individus à partir, par exemple, de sites de tatoueurs ou encore des informations collectées sur les réseaux sociaux des personnes concernées qui postent des photos en libre accès révélant leurs tatouages (ex. Instagram). La collecte de ce type de données prête à controverse à deux égards. En premier lieu, cet élément propre à un individu peut s'avérer unique selon le motif ou encore l'emplacement et l'étendue du tatoo (ex. une personne dont la tête est entièrement tatouée serait aisément identifiable par sa rareté). En deuxième lieu, un tatouage ne permet pas seulement d'identifier une personne mais peut aussi comporter d'autres informations sur l'individu (religion, opinions politiques, culture, croyances).

surtout des finalités de leur collecte). En outre, la collecte et l'analyse des indices visuels et des interactions sociales demeurent sujettes à interprétation. Enfin, l'analyse contextuelle d'images de caméras de surveillance nécessite une très grande quantité de données d'apprentissage et d'entraînement (mise en situation). Or, les chercheurs et industriels font souvent face à une insuffisance de données le plus souvent en raison de droit de propriété intellectuelle ou de droit au respect de la vie privée.

256. Les potentialités des usages de caméras « augmentées » filmant la voie publique sont multiples selon les finalités auxquelles elles se destinent ainsi que le type de données qu'elles sont amenées à traiter. Néanmoins, il convient de nuancer le propos car si les chercheurs en informatique et concepteurs d'algorithmes sont en mesure de traiter une grande diversité de données, ces technologies ne sont pas nécessairement destinées à la conception de caméras « augmentées ». Une étude prospective de l'emploi des différents types de caméras « augmentées » en France vise davantage à anticiper les enjeux afin de mettre en œuvre des normes et des règles explicites à destination des acteurs publics comme privés. Les premières caméras « augmentées » de sécurité publique ont vu le jour à l'étranger (ex. aux États-Unis, au Royaume-Uni ou encore en Chine) et ont engendré de vifs débats entourant les enjeux tant juridiques qu'éthiques, particulièrement lorsqu'elles ont été mises en œuvre en vue de « prédire » les agissements de personnes susceptibles de commettre une infraction[659]. La France s'est elle-aussi lancée dans la course aux caméras « augmentées » de vidéoprotection mais n'en est qu'à ses prémices.

B. Les algorithmes « augmentés » à des fins de sécurité publique : les usages en matière de caméras « augmentées » de sécurité publique

257. Les algorithmes « augmentés » d'aide à la prise de décision se sont progressivement imposés au sein des politiques de lutte contre les infractions[660]. Les algorithmes « augmentés » utilisés par les forces de l'ordre françaises sont aujourd'hui principalement destinés au ciblage de lieux propices à la commission d'infractions tels que les logiciels développés en interne de *Predvol* ou encore *Paved* (2). Pour l'heure, l'usage d'outils algorithmiques (internes ou commerciaux) « augmentés » de lutte contre les infractions portant directement sur des personnes (observation de

[659] Voir en ce sens : ARTE THEMA, « Prédire les crimes », *ARTE*, 2017, diffusé le 2 octobre 2018 [Documentaire disponible en ligne] ; McCABE (D.), "NOVA : Prediction by the Numbers" [2018], 52 min [Documentaire sur Netflix].

[660] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 68.

foules ou suivis d'individus) s'est systématisé principalement au sein des forces de l'ordre de certains pays étrangers. Parmi l'ensemble de ces pays, les États-Unis présentent différents cas d'usage intéressants de cette technologies (1).

1. L'usage des algorithmes « augmentés » par les forces de l'ordre aux États-Unis

258. Les usages d'algorithmes « augmentés » à des fins de sécurité publique portant sur les personnes sont multiples. L'exemple le plus emblématique est celui de Chicago, dans l'État de l'Illinois aux États-Unis, où les forces de l'ordre ont recours, depuis une dizaine d'années, à un logiciel appelé *Strategic Subject List* (SSL). Il permet de lister les personnes les plus susceptibles de commettre une infraction et d'identifier les individus sur lesquels les forces de l'ordre doivent se concentrer afin de prévenir les violences[661]. Face à la croissance fulgurante du nombre des données issues des caméras de surveillance et autres capteurs ainsi que celles collectées sur les réseaux sociaux dont disposaient les forces de l'ordre, ceux-ci se sont trouvés submergés par la quantité de données les rendant inexploitables. L'objectif du logiciel *SSL* consiste donc à aider les forces de l'ordre à identifier les éléments sur lesquels ils doivent focaliser leur attention.

259. La conception et l'usage de ce type d'algorithmes ciblant les personnes prêtent à controverse. Bien que le logiciel *SSL* exclut des données d'apprentissage issues des antécédents pénaux, de la race et du sexe, force est de constater que « plus de 400 000 citoyens de Chicago sont sur cette liste dont 1400 jeunes hommes considérés à haut risque »[662]. Aussi, les principales critiques émises à l'encontre de ce dispositif concernent aussi bien les critères permettant d'attribuer le « score de risque » des individus que son efficacité concrète face à la violence criminelle. De fait, pour freiner la criminalité, un ensemble de mesures doit être mis en œuvre en complément, notamment qu'en matière sociale, d'éducation, de santé ou encore économique. À cet égard, un autre type de logiciel de police « prédictive » utilisé à la Nouvelle-Orléans appelé *NOLA for Life* (*New Orleans' Youth Violence Prevention Plan*)[663] a visé à prévenir les violences chez les jeunes en associant un algorithme de détection des personnes susceptibles de commettre des infractions à des programmes d'aides sociales et économiques. Toutefois, ce logiciel n'aurait pas été développé en

[661] *Idem*, pp. 28-30 ; ARTE THEMA, « Prédire les crimes », *op. cit.*. Le logiciel après avoir été testé durant l'année 2012 sera finalement mis en service en 2013.

[662] CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 29.

[663] City of New Orleans' Youth Violence Prevention Plan [en ligne] consulté le 15 mars 2023.

interne mais en partenariat avec la société *Palentir*[664]. Cette révélation dans la presse avait soulevé des controverses quant au manque de transparence de la conception et de l'usage de ce logiciel ainsi que d'atteinte au droit à la vie privée. En conséquence, le maire de la ville n'avait pas renouvelé son partenariat avec la société *Palentir* la même année[665].

260. Les forces de l'ordre ont ainsi déjà eu recours à des outils algorithmiques d'IA issus d'entreprises privées afin d'effectuer un ciblage des personnes susceptibles de commettre des actes délictuels ou criminels. Aux États-Unis, l'outil *Beware*, développé par la société *Intrado*, est utilisé par les forces de l'ordre dans plusieurs villes depuis 2012[666]. Il s'agit d'une application mobile qui permet d'informer rapidement les agents en agrégeant des données contextuelles des appels d'urgence à des données publiques (commerciales et réseaux sociaux) ainsi que des données pénales[667]. L'algorithme de l'outil *Beware* attribue un score en fonction du niveau de risque que présentent les personnes entrant dans le cadre de l'enquête en cours[668]. Son utilisation reste toutefois controversée compte tenu du grand nombre de données, principalement à caractère personnel, sur lesquelles repose le fonctionnement de l'algorithme et de l'absence de démonstration de son efficacité[669].

261. L'intention à l'origine de l'élaboration de certains algorithmes « augmentés » laisse songeur. Le constat de voir plusieurs entreprises, françaises comme étrangères, adapter leurs technologies, habituellement destinées à des fins d'opérations militaires, à des activités de sécurité sur le territoire national suscite des interrogations de proportionnalité des usages technologiques[670].

---

664 WINSTON (A.), "Palantir has secretly been using New Orleans to test its predictive policing technology", *The Verge*, February 27th 2018 [en ligne] consulté le 15 mars 2023.

665 BULLINGTON (J.) and LANE (E.), "New Orleans ends its relationship with tech firm Palantir, Landrieu's office says", *NOLA.com | The Times-Picayune*, March 14th 2018 (updated on July 12th 2019) [en ligne] consulté le 15 mars 2023.

666 SMITH (M.), "Beware: Surveillance software police are using to score citizens' threat level", *CSO*, January 11th 2016 [en ligne] ; FRIEDERSDORF (C.), "A Police Department's Secret Formula for Judging Danger", *The Atlantic*, January 13th 2016 [en ligne].

667 CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 27.

668 VAN SCHENDEL (S.), "Risk Profiling by Law Enforcement Agencies in the Big Data Era: Is there a Need for Transparency?", pp. 275-289 *in* KOSTA (E.), PIERSON (J.), SLAMANING (D.), FISCHER-HÜBNER (S.), KRENN (S.). *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Vienna, Springer International Publishing, August 20-24th 2018 [en ligne sur HAL].

669 CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 27.

670 *Idem*, p. 7.

L'entreprise américaine *Palantir* fait notamment partie des pionnières en matière de conception d'outils, originairement d'usage militaire, à des fins policières pour lutter contre la criminalité. En ce sens, les ambitions des forces de l'ordre américaines semblent s'inspirer de certains projets à usage militaire tel que le projet *Maven*, développé aux États-Unis, dont les algorithmes d'IA reposent sur l'analyse des images issues de caméras fixées sur des drones aériens[671]. Mais le recours à d'autres algorithmes d'IA à des fins d'analyse d'images issues de caméras (fixes ou mobiles) filmant la voie publique ont également vu le jour en dehors du contexte militaire. À titre d'exemple, le *New York's Domain Awarness System*, un logiciel connecté à 6000 caméras de surveillance[672], serait capable d'analyser un grand nombre d'images vidéo de personnes qui sont ensuite interconnectées avec des données des services de police afin de les suivre notamment à l'aide d'éléments d'individualisation (vêtements ou objets en leur possession)[673].

262. Aujourd'hui, l'association d'algorithmes « augmentés » aux systèmes de vidéoprotection est en plein essor, en France comme à l'étranger, au point que certaines villes ont déjà commencé à expérimenter ces nouveaux dispositifs en vue d'améliorer la détection et la poursuite des auteurs d'infractions ou encore de prévenir les accidents[674].

2. L'usage des algorithmes « augmentés » par les forces de l'ordre en France

263. En France, plusieurs expérimentations et recours à des caméras « augmentées » ont eu lieu au sein de l'espace public[675]. Certaines expérimentations requéraient le traitement de DACP,

---

671 Voir notamment : CONGER (K.) and CAMERON (D.), "Google Is Helping the Pentagon Build AI for Drones", *gizmodo.com*, March 6th 2018 [en ligne] ; CHARTIER (M.), « Project Maven : le Pentagone signe pour 50 millions de dollars de contrats avec Amazon et Microsoft », *Les Numériques*, 9 septembre 2021 [en ligne] ; SERMONDADAZ (S.), « Projet Maven : Google met fin à son partenariat avec le Pengatone américain », *Sciences et Avenir*, 6 juin 2018 [en ligne] consultés le 22 mars 2023.

672 STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit.*, pp. 9-10.

673 FRANCESCANI (C.), "NYPD expands surveillance net to fight crime as well as terrorism", *Reuters*, June 21st 2013 [en ligne] consulté le 22 mars 2023.

674 Ministère de l'Économie, des Finances et de la Relance, « Rapport - Intelligence artificielle : État de l'art et perspectives pour la France », février 2019, p. 146. [en ligne].

675 CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », *op. cit.* ; CNIL « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », *cnil.fr*, 17 juin 2020 [en ligne] ; Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, *JORF* n°0060 du 11 mars 2021 [en ligne]. Voir aussi : Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, pp. 42-44 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), op. cit., pp. 33-34.

notamment des données biométriques (ex. traits du visage à des fins de reconnaissance faciale[676]), d'autres des données non identifiantes (ex. détection de présence ou de mouvement à des fins de détection d'anomalies ou de situations à dangereuses). Dès lors, ces caméras ne répondent pas toutes aux mêmes finalités et la conséquence des résultats fournis par leurs algorithmes diffère sensiblement. Aussi, il importe de distinguer les fonctions de l'algorithme selon les pays.

264. À l'inverse des États-Unis, la France n'a pas recours à des algorithmes de « prédiction » des évènements mais à des algorithmes d'aide à la prise de décision qui permettent de maintenir l'être humain dans la prise de décision. Ces algorithmes « augmentés » utilisés par les forces de l'ordre françaises ont ainsi vocation à apporter des éléments de réponse à un problème plutôt que de produire une solution complète à une solution donnée. Néanmoins, l'assistance pourvue par ces systèmes de traitement automatisé de données n'est pas sans conséquence sur la prise de décision des agents (v. **n° 781**). Les algorithmes « augmentés » d'aide à la prise de décisions associés aux caméras de vidéoprotection se scindent principalement en deux catégories : ceux destinés à l'identification de situations de danger et ceux ayant pour objectif le suivi de personnes suspectées d'avoir commis une infraction. Ces caméras « augmentées » d'aide au suivi de personnes peuvent avoir pour finalité l'identification ou l'authentification de personnes effectué soit au moyen d'un traitement de données biométriques[677] (ex. visage, iris, voix ou encore la démarche[678]) soit au moyen d'autres données telles que des vêtements ou objets distinctifs.

265. Aussi, des technologies de reconnaissance faciale ont déjà fait l'objet d'expérimentations sur la voie publique. En 2019, des caméras effectuant une reconnaissance faciale en temps réel avaient été déployées lors du carnaval de Nice au sein de l'espace publique à des fins expérimentales. Le cadre expérimental de cette technologie était limité à un évènement précis (le carnaval) et à une durée déterminée (durée de l'évènement). En outre, la licéité du traitement de données biométriques lors de cette expérimentation reposait sur une des exceptions prévues par le

---

676 Concernant les usages d'algorithmes de reconnaissance faciale en France en 2019 dans deux lycées, voir : TA Marseille, 9ème ch., 3 février 2020, n° 1901249 [en ligne] ; CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », *op. cit.*

677 L'analyse de données biométriques consiste à traiter et à mesurer des « éléments de la personne humaine suffisamment uniques et permanents pour présenter un bon degré de fiabilité dans la reconnaissance d'un individu » (Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 30).

678 « Les dernières recherches scientifiques tendent vers l'exploration d'autres caractéristiques biométriques telles que la voix, la démarche ou l'odeur corporelle » (Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 30).

RGPD à savoir le consentement des personnes concernées[679] qui se portaient volontaire pour participer à l'expérience. Une expérimentation similaire a été menée en 2020 lors de la compétition de Rolland Garros et avait également pour base légale le volontariat[680].

266. Il existe d'autres formes de caméras « augmentées » de sécurité publique, telles que celles destinées à la détection de situations de danger[681], aussi désignées sous le nom de « dispositifs d'alerte », qui consistent à assurer une surveillance de la voie publique « moins aléatoire et davantage ciblée sur des signaux objectifs d'anormalité »[682]. Ces algorithmes ont pour objectif d'émettre des signaux d'alertes lorsqu'ils détectent certains évènements qu'ils ont été entrainés à détecter (ex. bagages abandonné, accélération du mouvement d'une foule, etc.) et pourraient être en mesure de caractériser ces évènements[683]. Ces caméras visent principalement à analyser des évènements ayant cours dans des lieux spécifiques plutôt que d'analyser les situations individuelles[684]. Aussi, certaines caméras « augmentées » d'identification de situations de danger peuvent reposer sur un traitement de DACP[685] sans toutefois procéder à un traitement de données

---

679 RGPD, art. 9, al. 2 a).

680 À noter que cette expérimentation a eu lieu lors de l'année de la pandémie du COVID-19 où le nombre de spectateurs admis était limité dans les lieux de compétition afin de respecter les mesures de sécurité sanitaire. Secrétariat générale de la défense et de la sécurité nationale (SGDSN), « Anticiper les risques et les menaces », 22 novembre 2022 [en ligne] consulté le 11 avril 2023. Voir aussi : LE FOLL (C.) et POURÉ (C.), « Thales à Roland-Garros : têtes et match », *Les Jours*, 9 novembre 2021 [en ligne] consulté le 12 avril 2023.

681 Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 23-25 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, Annexe 9, pp. 290-291 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

682 Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, p. 72.

683 À titre d'exemple, la crise sanitaire due à la pandémie de COVID-19 a été propice à l'usage de caméras « augmentées » collectant différents types de données à des fins de gestion de la propagation du virus telles que les caméras « thermiques » ou encore les caméras de détection du port du masque à des fins statistiques. Voir notamment : CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », *op. cit.* ; CNIL, Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports [en ligne].

684 Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 23.

685 À noter que la qualification de DACP peut parfois poser des difficultés. Ce fut notamment le cas lorsqu'en 2019 la ville de Saint-Étienne avait expérimenté un dispositif de captation et d'analyse de sons de la voie publique. Les micros posés au sein de l'espace public avaient pour objectif de capter des bruits suspects tels que des cris, du verre brisé, des klaxons, des crépitements ou des coups de feu puis de les analyser par comparaison aux modèles pré-enregistrés de l'algorithme (Voir notamment : « St Etienne : des capteurs sonores à l'écoute de la ville », 1er mars 2019 [en ligne]). Cet usage avait été contesté par la CNIL via une lettre de sa présidente qui craignait que des données biométriques puissent être collectées et rappelait qu'aucune base légale n'existait pour encadrer cet usage (Lettre de la présidente de la CNIL au président de Saint-Étienne métropole le 25 octobre 2019 [en ligne]). Suite à cette intervention de la CNIL, la ville de Saint-Étienne avait cessé le déploiement de ce dispositif dans l'espace public.

biométriques. Enfin, il convient de rappeler que le suivi d'un individu pourrait être effectué à partir d'autres données telles que les vêtements ou un signe distinctif (ex. coiffure, tatouage, etc.).

267. Les flux et regroupements de personnes (principalement lors de manifestions sportives, culturelles ou politiques) sont susceptibles d'engendrer des atteintes à l'ordre public ou d'être la cible d'attaques à caractère terroriste. Face à la massification des images de vidéoprotection et des besoins que suscite la gestion de grands évènements, ces caméras « augmentées » présentent une opportunité d'aide aux forces de l'ordre et aux services de secours. Ces derniers pourraient bénéficier des remontées d'alertes de ces dispositifs afin d'adapter le déploiement de leurs moyens humains et techniques. Le recours à des drones aériens « augmentés » de sécurité publique présente un avantage supplémentaire par leur caractère mobile dans les situations où les caméras fixes s'avèreraient insuffisantes. Les résultats obtenus lors des expérimentations au sein de l'espace public et les besoins que requière la sécurisation des JOP de 2024 à Paris ont conduit les autorités publiques à prévoir l'usage de cette technologie[686].

268. L'ambition des forces de l'ordre et des services de secours de recourir à des caméras (fixes ou aéroportées) « augmentées » filmant la voie publique fait cependant face à une absence d'encadrement permettant d'apporter des garanties suffisantes des droits et libertés. La CNIL n'a pas manqué de rappeler l'inadéquation du cadre juridique actuel pour envisager l'emploi d'une technologie qui « ne constitue pas le prolongement des dispositifs [de vidéoprotection] existants mais un changement de nature »[687].

§2. La nécessité d'un encadrement juridique adapté aux algorithmes « augmentés » à l'usage de la sécurité publique

269. La recherche constante de réponses aux besoins en matière de sécurité publique a suscité un recours de plus en plus fréquent à des algorithmes « augmentés ». Bien que ces progrès technologiques présentent un sérieux potentiel d'amélioration des activités de sécurité publique, les agents vont devoir s'adapter à ces nouveaux usages (v. **n° 783 et suiv.**). Aussi, le recours aux algorithmes « augmentés », particulièrement dans un cadre régalien, suscite de nombreuses

686 SGDSN, « Anticiper les risques et les menaces », *op. cit.* ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, Annexe 9, p. 291.

687 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 5 et p. 18.

controverses majoritairement liées au manque de transparence et d'explicabilité de leur fonctionnement[688]. Il en va ainsi particulièrement concernant le domaine de la surveillance de l'espace public qui repose essentiellement sur des motifs davantage préventifs que répressifs, engendrant un climat de suspicion général et portant inévitablement atteinte à la confiance des individus envers la force publique[689].

270. L'introduction de cette technologie au sein des forces de l'ordre vient répondre aux attentes formulées depuis plusieurs années par le ministère de l'Intérieur en faveur d'une modernisation des outils de sécurité en vue de la gestion des données massivement collectées. Face à l'absence d'un cadre juridique spécifique à l'usage des algorithmes, il invitait à la mise en œuvre « d'un *corpus* législatif adapté aux données d'apprentissage (constitution, conservation, exploitation, supervision des jeux de données) [qui] servirait au développement des systèmes d'IA pour les services de police (judiciaire, sécurité publique) et les partenaires du *continuum* ainsi qu'à la fiabilisation de ces outils pour le respect des libertés »[690].

271. En matière de surveillance de la voie publique, les forces de l'ordre doivent faire face à un afflux conséquent de données à traiter. L'explosion du nombre de caméras filmant la voie publique aura eu pour double effet d'augmenter le champ de la surveillance des forces de l'ordre mais d'empêcher en contrepartie les agents de visualiser en direct l'ensemble des images captées par ces caméras[691]. Pour y remédier les autorités souhaitent avoir recours à des technologies algorithmiques avancées, en d'autres termes à des technologies d'IA. Ces technologies se sont présentées ces dernières années comme prometteuses et permettraient, dans le cadre d'une utilisation associée à des caméras de vidéoprotection, d'analyser et d'interpréter les nombreuses

---

[688] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, spéc. pp. 69-80 ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, spéc. pp. 126-127 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 14-17.

[689] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 16.

[690] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*, pp. 9-10.

[691] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 58 : « Malheureusement, un agent chargé de la surveillance de nombreuses caméras ne peut tout observer ». De fait, un être humain « est incapable d'observer instantanément toutes les images de vidéoprotection afin de détecter des menaces potentielles, en revanche l'intelligence artificielle le peut ».

images[692].

272. Ces dernières années, la CNIL a pu constater l'augmentation du nombre de dispositifs de vidéoprotection équipés de logiciel d'IA (ou « caméras augmentées ») au sein de l'espace public[693]. Ces observations ont été confirmées par les nombreuses saisines dont elle a fait l'objet, notamment dans le cadre de projets de recherche impliquant des acteurs privés comme publics[694]. La multiplication de ces dispositifs serait la conséquence d'intérêts privés comme publics motivés par des enjeux industriels, économiques mais aussi politiques dans le cadre de la stratégie de numérisation de l'État[695]. Sur ce sujet la CNIL a publié des travaux portant sur la problématique des villes intelligentes intégrant des dispositifs de caméras augmentées et des enjeux tant éthiques que juridiques engendrés par le recours aux algorithmes d'IA[696]. Elle a par la suite confirmé ses inquiétudes concernant l'introduction de caméras « augmentées » au sein de l'espace public sans aucun cadre juridique adéquat et appelait à un débat démocratique permettant la mise en œuvre d'une législation adaptée[697].

273. Les caméras de vidéoprotection fixes comme mobiles disposent désormais d'un cadre juridique qui leur est spécifique. De manière similaire, les algorithmes « augmentés » à des fins de sécurité publique nécessitent un encadrement juridique adapté qui permette de répondre aux enjeux qu'ils soulèvent[698]. En France, l'encadrement des algorithmes se limite à la loi pour une République numérique du 7 octobre 2016[699]. Toutefois, certains algorithmes effectuent des traitements portant

---

[692] *Ibid.*

[693] DROIN (A.), DUBOYS FRESNEY (M.), MAULIN (C.) et VINCENT (A.), « Actualité Informatique et Libertés - Déploiements de caméras "augmentées" : sous quelles conditions ? », *AJDA* n° 39, 21 novembre 2022, p. 2223 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

[694] À l'image des projets ANR S2UCRE, ANR GIRAFE et FUI COOPOL.

[695] Voir notamment : Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*

[696] LINC-CNIL, Cahier IP n° 5 « La plateforme d'une ville - Les données personnelles au coeur de la fabrique de la smart city », *linc.cnil.fr,* septembre 2017, p. 39 [en ligne] ; CNIL, Rapport de synthèse du débat public animé par la CNIL sur les enjeux éthiques des algorithmes et de l'intelligence artificielle « Comment permettre à l'Homme de garder la main ? - Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.*

[697] CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », *op. cit.*

[698] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.* ; MATTATIA (F.), « Expérimentation de caméras intelligentes pour les JO de 2024 : quel encadrement juridique ? », *JCP A* n° 4, 30 janvier 2023, 2028.

[699] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n°0235 du 8 octobre 2016 [en ligne].

sur des DACP et sont par conséquent soumis à la règlementation relative à ces données (RGPD, DPJ et LIL). Cependant, aucun cadre juridique spécifique à la conception et à l'usage des algorithmes « augmentés » n'a encore été adopté.

274. Face aux multiples enjeux que soulèvent l'IA et les algorithmes dans les différents secteurs, les autorités européennes ont pris la décision d'élaborer une Proposition de Règlement, à l'initiative de la Commission européenne, visant à établir des règles harmonisées en matière d'Intelligence artificielle publiée le 21 avril 2021[700] (REIA). En dépit des avancées en matière d'encadrement juridique des systèmes d'IA (SIA) qu'offre ce texte, celui-ci a rapidement fait l'objet de nombreuses critiques soulignant ses lacunes, particulièrement en matière de protection des droits et libertés[701]. Les principales critiques visaient notamment les usages en matière de police et de justice à l'image de la résolution du Parlement européen émise le 6 octobre 2021[702] par laquelle ce dernier adopte une position sensiblement plus protectrice des droits et libertés[703]. L'adoption du texte nécessitait par conséquent la révision de plusieurs des dispositions initiales du REIA (A).

275. Ces initiatives européennes, bien que salutaires, ne sont qu'un pas en faveur d'une règlementation à l'usage des caméras « augmentées » de vidéoprotection. La souveraineté des États impose de devoir mettre en œuvre un cadre plus spécifique applicable à cette technologie utilisée dans un cadre régalien. Pour faire face aux ambitions d'utilisation par les forces de l'ordre et les services de secours d'algorithmes d'analyse d'évènements associés à des systèmes de vidéoprotection lors des Jeux Olympiques et Paralympiques prévus à Paris en 2024 (JOP2024), le

---

700 Commission européenne, « Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle et modifiant certains actes législatifs de l'Union) », 21 avril 2021, *op. cit.* À noter que le texte du règlement européen pour l'Intelligence artificielle (REIA) est souvent désigné par l'abréviation anglo-saxonne *AI Act* par les membres de la doctrine.

701 De manière non-exhaustive : EDPB, Avis conjoint 05/2021 de l'EDPB et du CEPD sur « la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), 18 juin 2021 [en ligne] ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022, *op. cit.* ; CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, 7 avril 2022, *op. cit.* ; CRICHTON (C.), « Prudence du Parlement européen sur l'utilisation de l'IA par les autorités policières et judiciaires », *Dalloz IP/IT* n° 11, 24 novembre 2021, p. 538 ; CASTET-RENARD (C.), « Quel droit de l'intelligence artificielle dans l'Union européenne ? Ou les multiples ambitions normatives de l'*AI Act* », *Dalloz IP/IT* n° 2, 19 février 2022, p. 67 ; BOINE (C.), Les systèmes d'intelligence artificielle à finalité générale et la proposition de règlement de la Commission européenne », *Dalloz IPT/IT* n° 2, 19 février 2022, p. 79 ; MATHIS (B.), « Proposition de règlement européen sur l'intelligence artificielle : le regard d'un praticien », *RLDI* n° 192, mai 2022, pp. 40-44.

702 Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », 6 octobre 2021, *op. cit.*

703 CRICHTON (C.), « Prudence du Parlement européen sur l'utilisation de l'IA par les autorités policières et judiciaires », *op. cit.*

législateur français a mis en œuvre un texte afin d'encadrer leur utilisation à titre expérimental. Ces dispositions - provisoires - entendent répondre aux exigences formulées par les autorités protectrices des droits et libertés afin d'encadrer au mieux l'utilisation de caméras « augmentées » lors des JOP 2024. En tous les cas, le législateur devra définir un cadre adapté à la conception ainsi qu'à l'usage des algorithmes « augmentés » de sécurité publique, notamment ceux associés aux systèmes de vidéoprotection (B).

A. L'encadrement supranational des algorithmes « augmentés » : les espoirs suscités par la règlementation européenne pour l'IA

276. Il convient de saluer l'initiative européenne visant à mettre en œuvre un cadre juridique général à l'usage des algorithmes d'IA ou SIA. Par cette démarche, les institutions européennes font office de pionnières en matière d'encadrement de la conception et de l'utilisation de ces technologies[704] (1). Sans le REIA seules les dispositions du RGPD et de la DPJ relatives à l'utilisation des algorithmes[705] permettent leur encadrement. Toutefois, ces rares dispositions ne concernent que les algorithmes chargés de rendre des décisions « automatiques » à partir de DACP et sont limitées à certains usages. Il était donc nécessaire d'établir un cadre juridique général centré sur la conception et l'usage des algorithmes « augmentés » notamment d'aide à la prise de décision. Pour autant, les dispositions du REIA ont rapidement fait l'objet de nombreuses critiques (2).

1. Les promesses du REIA pour encadrer les algorithmes « augmentés »

277. Afin de faire face aux nouveaux enjeux juridiques que suscitent l'arrivée des SIA, les institutions européennes ont engagé leur réflexion et remis des rapports visant à évaluer leurs effets dans différents domaines. Tout d'abord, le Conseil de l'Europe, au travers de sa Commission européenne pour l'efficacité de la justice, a publié une Charte éthique européenne d'utilisation de l'IA dans les systèmes judiciaires et leur environnement le 4 décembre 2018[706]. Cette Charte

---

[704] Le texte du REIA constitue l'un des premiers cadres juridiques mondiaux portant spécifiquement sur la conception et l'utilisation de l'IA. FÉRAL-SCHUHL (C.) et SINIBALDI (J.), « Un cadre juridique européen pour l'intelligence artificielle : une première mondiale ! », *feral.law*, 15 novembre 2021 [en ligne] ; Mc DONALD (B.), « L'Union européenne en passe de devenir un leader mondial dans l'IA éthique », *journaldunet.com*, 9 mars 2023 [en ligne] consultés le 10 mars 2023.

[705] RGPD, art. 22, cons. 71 et 72 ; DPJ, art. 11.

[706] Conseil de l'Europe, « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ), 3-4 décembre 2018, 84 p. [en ligne].

éthique comprend plusieurs principes « piliers » en matière de conception et d'usage des algorithmes mais se concentre plus spécifiquement sur les enjeux relatifs à la « justice prédictive ». Particulièrement soucieux des risques engendrés par l'utilisation des SIA[707], le Conseil de l'Europe a, par la suite, rédigé des recommandations concernant l'incidence de leur utilisation sur les droits de l'Homme[708] qui ont été publiées en avril 2020.

278. L'Union européenne a également contribué à une réflexion assez générale sur le développement et les usages de l'IA en publiant plusieurs textes qui ont servi de base à l'élaboration du REIA. Dans le même esprit que le Conseil de l'Europe, la Commission européenne avait rédigé des lignes directrices en matière d'éthique de l'IA appliquée à la justice le 9 avril 2019[709]. Début 2020, elle avait apporté de nouvelles recommandations en matière d'IA au travers du « Livre blanc Intelligence artificielle »[710]. En octobre 2020, le Parlement européen avait poursuivi les efforts dans la recherche d'un cadre juridique de l'IA et des algorithmes en publiant une résolution en matière d'IA[711]. En avril 2021, la Commission européenne a publié sa proposition de règlementation de l'IA. Par la suite, le texte a fait l'objet de négociations, afin de répondre aux écueils soulignés par différentes organisations, qui ont abouti à un compromis adopté par le Parlement européen le 11 mai 2023 proposant un nouveau cadre juridique pour l'IA (Amendement REIA)[712]. Le Conseil européen et le Parlement européen sont parvenus a un accord sur le texte du REIA le 9 décembre 2023[713],

---

[707] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance, 31 mars 2022, *op. cit.*, (Annexe 10) p. 359.

[708] Comité ministériel du Conseil de l'Europe, « Recommandation aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme », CM/Rec(2020)1, *op. cit.*

[709] Commission européenne, « Lignes directrices en matière d'éthique pour l'IA », *op. cit.*

[710] Commission européenne COM(2020) 65 final, « Livre blanc Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance », *op. cit.*

[711] Parlement européen, « Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes », *op. cit.*

[712] European Parlement,"Draft Compromise Amendments - Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", May 9th 2023, 144 p. [en ligne].

[713] Conseil de l'Union européenne, « Législation sur l'intelligence artificielle: le Conseil et le Parlement parviennent à un accord sur les premières règles au monde en matière d'IA », 9 décembre 2023 [en ligne].

suite à l'amendement publié en mai 2023[714]. Cependant, le texte doit encore faire l'objet de quelques ajustements et être présenté aux États membres avant d'être définitivement adopté[715].

279. Au niveau international, l'Organisation des Nations Unies (ONU) se préoccupe elle aussi des conséquences que peuvent avoir l'introduction massive des technologies basées sur l'IA. L'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) est parvenue à mettre en œuvre des principes éthiques généraux internationaux pour ces technologies en adoptant le premier accord pour l'éthique de l'IA[716]. Celui-ci introduit une définition volontairement étendue de l'IA[717] et repose principalement sur quatre axes que sont la protection des données, l'interdiction de la notation sociale et de la surveillance de masse, l'aide au suivi et à l'évaluation des SIA, et la protection de l'environnement. En mai 2023, le G7 a également fait part de son ambition de créer un groupe de travail autour des sujets liés au développement de l'IA afin d'établir des mesures permettant leur encadrement pour un usage « responsable »[718].

280. Outre le REIA, les principes issus de la Conv.EDH et de la CDFUE sont applicables aux algorithmes d'IA, notamment le droit au respect de la vie privée[719] et à la protection des données à caractère personnel[720], la liberté d'aller et venir[721], la liberté d'expression[722], le droit à la liberté et à la sûreté[723] ou encore le principe de non-discrimination[724]. De manière générale, les institutions

---

[714] European Parlement, Press release "AI Act: a step closer to the first rules on Artificial Intelligence", May 11th 2023 [en ligne] consulté le 11 mai 2023.

[715] Conseil de l'Union européenne, « Législation sur l'intelligence artificielle: le Conseil et le Parlement parviennent à un accord sur les premières règles au monde en matière d'IA », *op. cit.*

[716] UNESCO, « Recommandation sur l'éthique de l'intelligence artificielle », 2022, 43 p. [en ligne] ; UNESCO, « UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence », 25 November 2021 [en ligne].

[717] L'UNESCO y définit l'IA comme tous « systèmes capables de traiter les données et l'information par un processus s'apparentant à un comportement intelligent, et comportant généralement des fonctions de raisonnement, d'apprentissage, de perception, d'anticipation, de planification ou de contrôle ».

[718] MAZHAR (S.), « Intelligence artificielle : Le G7 travaille sur une "utilisation responsable" », *ladepeche.fr*, 22 mai 2023 [en ligne] ; SMIALOWSKI (B.), « Le G7 établit un protocole sur l'IA pour lutter contre la désinformation », *i24news*, 20 mai 2023 [en ligne] consultés le 22 mai 2023.

[719] Conv.EDH, art. 8 ; CDFUE, art. 7.

[720] Conv.EDH, art. 8 ; CDFUE, art. 8.

[721] Conv.EDH, art. 8 ; CDFUE, art. 6.

[722] Conv.EDH, art. 10 ; CDFUE, art. 11.

[723] Conv.EDH, art. 5 §1 ; CDFUE, art. 6.

[724] Conv.EDH, art. 14 et Protocole 12, art. 1er.

supranationales insistent sur l'obligation des États membres de faire respecter les droits de l'homme[725] par les concepteurs et les utilisateurs de SIA et s'accordent sur le besoin d'avoir un cadre législatif et réglementaire qui leur soit adapté[726]. Dès lors, le REIA constitue une avancée considérable dans l'objectif d'assurer le contrôle des différents SIA.

281. À l'instar des règles européennes adoptées concernant l'usage de drones aériens au sein de l'espace aérien national, le REIA repose sur une approche visant à classifier les différents types de technologies d'IA en fonction des risques qu'elles peuvent présenter. Il introduit quatre catégories : « risque inacceptable », « risque élevé », « risque limité » et « risque minime »[727]. Les SIA considérés comme étant porteurs de menaces inacceptables pour les droits et les libertés des individus seront par conséquent interdits. Cette approche par les risques s'adaptera à l'usage « augmentés » des drones aériens de sécurité publique qui répondent déjà à une classification par les risques depuis la révision du règlement européen relatif à l'aviation civile de 2018 (v. **n° 161-163**). En dépit des nombreuses critiques et remaniements auquel aura fait face le REIA, le choix d'une classification par les risques des SIA semble être le plus adéquat.

2. Les limites du REIA pour encadrer les algorithmes « augmentés »

282. Les amendements adoptés par le Parlement européen dans son compromis voté le 11 mai 2023 entendaient répondre aux nombreux signaux d'alerte des organismes, publics comme privés, de protection des droits et libertés sur l'usage de certains SIA[728] notamment ceux ayant recours au traitement de données biométriques. En ce sens, il avait déjà formulé des réserves en octobre 2021

---

[725] Comité ministériel du Conseil de l'Europe, « Recommandation aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme », *op. cit.*, p. 2 ; Parlement européen, « Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes », *op. cit.*, cons. J.

[726] Dans sa recommandation du 8 avril 2020, le Comité des Ministres du Conseil de l'Europe rappelait aux États membres leur obligation « d'établir des cadres législatifs, réglementaires et de supervision efficaces et prévisibles, capables de prévenir, de détecter, d'interdire et de réparer les violations des droits de l'homme, que celles-ci soient imputables à des acteurs publics ou privés » (Comité ministériel du Conseil de l'Europe, « Recommandation aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme », *op. cit.*, p. 2).

[727] REIA, art. 3.

[728] CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, *op. cit.*, spéc. recommandation n°6 ; DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », *op. cit.* ; DDD, Avis établissant des recommandations et des principes essentiels pour la future législation européenne portant sur l'intelligence artificielle : « Pour une IA européenne protectrice et garante du principe de non-discrimination », 21 juin 2022 [en ligne] ; Voir aussi la lettre signée par plusieurs organismes de défenses des droits et libertés : "European Parliament: Make sure the AI act protects peoples' rights!", April 2023 [en ligne] ; EDRi (European Digital Rights), "Civil society urges European Parliament to protect people's rights in the AI Act", April 9th 2023 [en ligne].

s'agissant de la première version du texte du REIA concernant l'usage de SIA dans le cadre pénal[729]. À cette occasion, il avait formulé sa volonté de ne pas faire de l'utilisation des SIA une fin en soi et de conserver l'objectif du bien-être des êtres humains. Aussi, il avait rappelé que ces technologies devaient respecter tous les principes issus du droit pénal tels les principes de non-discrimination et de présomption d'innocence. Il estimait que, eu égard aux nombreuses DACP que les SIA utilisés à des fins pénales pouvaient traiter, ceux-ci devraient être - *a minima* - « sûrs, solides, sécurisés et adaptés à l'usage prévu »[730]. Dès lors, il souhaitait que ces technologies soient soumises à des contrôles stricts de proportionnalité[731] et que des garanties soient mises en œuvre en fonction des risques qu'ils engendraient pour les droits et libertés. Enfin, il avait réclamé un moratoire sur le développement et le recours aux systèmes de reconnaissance faciale à des fins pénales[732] le temps que soit adoptées des règles plus spécifiques en la matière.

283. Bien que le Parlement européen reconnaisse les nombreux avantages que confèrent les SIA dans le domaine pénal, il avait estimé qu'ils devaient être classés comme étant à « risque élevé » lorsqu'ils sont susceptibles « d'avoir une incidence significative sur la vie des personnes »[733]. En outre, il avait insisté sur la nécessité de mettre en œuvre des mesures de contrôle strictes et une surveillance indépendante. Enfin, le Parlement européen avait souligné un enjeu général évident tenant à l'asymétrie de pouvoir créé par les SIA utilisés à des fins pénales entre les personnes qui les utilisent et celles faisant l'objet de leur traitement[734].

284. Le Parlement européen n'a pas été seul à critiquer les dispositions originelles du REIA. Au premier rang, le Comité européen de protection des données (*EDPB*)[735] et le Contrôleur

---

729 Parlement européen, « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*

730 *Idem*, art. 4.

731 *Idem*, art. 25.

732 *Idem*, art. 27.

733 *Idem*, art. 5.

734 *Idem*, art. 10.

735 Le Comité européen de protection des données ou *European Data Protection Board* (CEPD/*EDPB*) est un organisme européen indépendant qui réunit les différentes autorités de protection de données des États membres de l'Union européenne. Le Contrôleur européen de la protection des données ou *European Data Protection Supervisor* (CEPD/*EDPS*) est l'autorité de contrôle indépendante des institutions européennes sur la protection des données.

européen de la protection des données (*EDPS*) ont émis un avis le 18 juin 2021[736]. En France, l'avis publié par la CNCDH sur l'incidence de l'IA sur les droits fondamentaux comprend des réflexions et des recommandations concernant le REIA. D'une manière générale, les différentes instances nationales et européennes estiment que ce texte constitue une solution prometteuse et essentielle afin d'encadrer la conception et l'usage des SIA dans le respect des droits et des libertés des personnes. Ils approuvent notamment l'approche fondée sur le risque du REIA et la création du « Comité européen de l'Intelligence artificielle » (CEIA). Leurs avis sont globalement favorables aux dispositions proposées mais soulignent cependant certaines lacunes et imprécisions[737].

285. D'une manière générale, les avis critiquent le caractère imprécis de la définition de la catégorie relative aux IA interdites et formulent le souhait d'un élargissement de son champ d'application. Les différentes instances souhaitent, à titre principal, que les exceptions à l'interdiction générale de recourir à l'identification biométrique à distance des personnes dans l'espace public soient supprimées du texte[738]. De même, elles considèrent comme hautement inacceptable le recours à des SIA visant à déduire les émotions d'une personne physique et estiment que ces usages devraient être interdits par principe[739]. Aussi, elles incitaient à une clarification du cadre des SIA (permises et interdites). Ensuite, ils souhaitaient que les dispositions du REIA s'articulent avec celles du RGPD et de la DPJ[740]. Enfin, s'agissant du CEIA, le Comité européen de protection des données souhaitait que les garanties concernant l'indépendance de ses membres et les pouvoirs de contrôle qui leur sont conférés soient renforcés[741].

286. Enfin, le REIA a également fait l'objet de critiques quant aux dispositions relatives au recours à des SIA par le secteur public. En France, la Direction générale des douanes regrettait que le texte créé des règles nettement plus strictes à l'encontre du secteur public car selon elle la

---

[736] EDPB, « Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) », *op. cit.* ; Voir également : CNIL, « Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen », 8 juillet 2021 [en ligne].

[737] CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux (Avis IA), *op. cit.*, p. 7 : « La Commission relève l'insuffisance des garanties propres à assurer un respect effectif de ces derniers ».

[738] EDPB, Avis conjoint 05/2021, *op. cit.*, (32), p. 14 ; CNCDH, Avis IA, *op. cit.*, (24) p. 12.

[739] EDPB, Avis conjoint 05/2021, *op. cit.*, (35), p. 14 ; CNCDH, Avis IA, *op. cit.*, (32) p. 15. Voir également en ce sens : DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », *op. cit.*

[740] EDPB, Avis conjoint 05/2021, *op. cit.*, (15) (22) (23), pp. 9 et 11.

[741] *Idem*, (51) (52), p. 18.

Commission européenne aurait estimé que « l'usage de l'IA dans le secteur privé mérite moins d'attention que son usage dans le secteur public »[742]. Cette affirmation serait de fait cohérente avec les signalements formulés sur les réseaux sociaux et les propos rapportés par la *Quadrature du Net* s'agissant de l'usage de caméras analysant des données biométriques dans des supermarchés[743]. En outre, le rapport du Sénat du 10 mai 2022 soulignait que les SIA classés comme étant à « haut risque » concernaient principalement ceux relevant de la puissance publique[744].

287. L'amendement au REIA, voté par le Parlement européen le 11 mai 2023, apporte des précisions quant au cadre d'utilisation des SIA notamment s'agissant du domaine pénal. Ces modifications ont été définitivement adoptées lors des débats du Parlement européen le 14 juin 2023[745]. Cette nouvelle version du REIA apporte des éclaircissements sur ce que pourraient contenir les textes nationaux en matière de caméras « augmentées » filmant la voie publique. Elles apportent en tout les cas un espoir de ne pas voir encore s'élargir le champ des potentialités de surveillance de l'espace public.

B. Les premiers pas vers un cadre national *ad hoc* applicables aux algorithmes « augmentés » utilisés à des fins de sécurité publique

288. Depuis plusieurs années, l'absence de dispositions spécifiques permettant l'encadrement des algorithmes « augmentés » a incité les professionnels du secteur à proposer des solutions d'IA de « confiance » par l'intermédiaire de guides d'éthiques à l'usage des concepteurs et des développeurs[746]. Ces chartes et guides éthiques visent notamment à « défendre un usage et un développement responsables et éthiques des technologies biométriques »[747]. Bien que les principes adoptés soient souvent en accord avec les droits de l'Homme, leur portée demeure toutefois limitée.

---

[742] Propos de la DGD rapportés par le Rapport d'information du Sénat n° 627, *op. cit.*, p. 49.

[743] La Quadrature du Net, « Vidéosurveillance biométrique dans nos supermarchés », *laquadrature.net*, 31 mai 2021 [en ligne]. Voir aussi : JUSQUIAME (T.), « Ils utilisent la surveillance algorithmique : Leclerc, Fnac, Biocoop et de nombreux commerces surveillent illégalement leurs clients », *Street Press*, 27 juin 2023 [en ligne] ; « Le vol à l'étalage fait le lit de la vidéosurveillance algorithmique », *NextInpact*, 28 juin 2023 [en ligne] consultés le 28 juin 2023.

[744] Rapport d'information du Sénat n° 627, *op. cit.*, p. 49.

[745] Parlement européen, P9_TA(2023)0236 Législation sur l'intelligence artificielle, 14 juin 2023 [en ligne].

[746] En France, de manière non exhaustive : Numeum (Syndicat professionnel des entreprises du numérique en France) a créé un guide pratique « Ethical IA » en septembre 2021 [disponible en ligne] ; l'Alliance pour la confiance numérique (ACN) a contribué à l'élaboration d'une charte éthique de la profession [en ligne] ; la société Thalès adopte une approche sous « TrUE » basée sur la traçabilité, l'intelligibilité et l'éthique [en ligne].

[747] Sénat, Rapport d'information n° 627, *op. cit.*, p. 49.

De fait, les différences entre les règles éthiques internes à chaque entreprise ne permettent pas d'apporter des garanties suffisantes et pourraient de surcroit susciter « un biais d'acceptabilité, qui pourrait conduire à desserrer la contrainte réglementaire et institutionnaliser »[748]. Suite à ce constat, différents rapports et études[749] ont été publiés par les institutions françaises afin de faire face à ces enjeux. Aussi, tenant compte de l'usage grandissant des SIA au sein du secteur public, certains de ces documents portent spécifiquement sur le sujet des algorithmes d'IA mis en œuvre par le secteur public[750]. Pour l'heure, les dispositions législatives et la jurisprudence ne permettent pas d'encadrer spécifiquement le développement et l'usage des algorithmes « augmentés » de sécurité publique (1). Néanmoins, le législateur s'est efforcé d'adopter des dispositions provisoires pour réglementer l'usage des caméras « augmentées » de sécurité publique lors des grands évènements prévus en France en 2023 et 2024 (2).

1. L'absence de règles juridiques adaptées à l'usage des algorithmes « augmentés » de sécurité publique

289. Le Conseil d'État est l'un des premiers à s'être intéressé à la question en consacrant son étude annuelle de 2014 au numérique et aux droits fondamentaux[751] qui évoquait les enjeux liés aux algorithmes produisant des effets juridiques lorsqu'ils traitent des DACP. À cette occasion, il avait appelé à la mise en œuvre d'un droit encadrant spécifiquement cette technologie. De fait, la LIL interdit en principe la prise de décision individuelle fondée exclusivement sur un algorithme[752]. Toutefois, le RGPD prévoit la possibilité pour les États membres de mettre en œuvre leurs propres

---

748 Propos de LEQUESNE-ROTH (C.) recueillis par le Sénat (Rapport n° 627, *op. cit.*, p. 50).

749 Voir notamment : Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.* ; Ministère de l'Économie, des Finances et de la Relance, « Rapport - Intelligence artificielle : État de l'art et perspectives pour la France », *op. cit.* ; CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, *op. cit.* ; Sénat, Rapport d'information n° 483 (2022-2023) fait au nom de la commission des affaires européennes « relatif à la proposition de législation européenne sur l'intelligence artificielle » remis par GATTOLIN (A.), MORIN-DESAILLY (C.), PELLEVAT (C.) et SCHALCK (E.), 30 mars 2023 [en ligne].

750 Voir notamment : Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.* ; Rapport au Premier ministre « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.* ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.* ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

751 CE, Étude annuelle sur « Le numérique et les droits fondamentaux », 9 septembre 2014 [en ligne].

752 RGPD, art. 22 ; LIL, art. 47 : « Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne ».

exceptions[753]. C'est ainsi que la LIL intègre une exception autorisant la prise de décisions administratives fondées exclusivement sur un traitement automatisé de DACP sous la condition que ces DACP n'appartiennent pas à la catégorie des données sensibles[754] au sens de l'article 9 du RGPD[755].

290. Face à l'utilisation croissante des algorithmes par l'État à des fins administratives, le Sénat s'était également inquiété de la dangerosité que représenteraient des décisions fondées exclusivement sur un algorithme de type « auto-apprenant » ayant pour conséquence de réviser les règles relatives au processus décisionnel. En ce sens, il avait formulé le souhait de conserver la présence d'un être humain dans le processus décisionnel final portant sur des individus[756]. Dans sa décision du 12 juin 2018[757], le Conseil constitutionnel avait été saisi de la question du recours à des algorithmes de type « auto-apprenant » et de leur incidence sur les droits et libertés constitutionnellement garantis. Sur ce point, il avait adopté une position en faveur des sénateurs requérants, en interdisant l'utilisation « comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement »[758].

291. Le recours à la prise de décision automatisée par l'État est donc limité et certains domaines ou secteurs l'interdisent de manière stricte. En ce sens, le Conseil constitutionnel avait déjà eu l'occasion, le 13 mars 2003[759], de préciser les usages portant sur la prise de décision automatisée[760] notamment dans le domaine de la police. Aussi, l'article 95 de la LIL[761] interdit par principe que des traitements de DACP à des fins pénales fassent l'objet d'une décision individuelle

---

[753] RGPD, art. 22 §2.

[754] LIL, art. 47 al. 2.

[755] RGPD, art. 22 §4.

[756] ROCHFELD (J.), « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* n°9, 12 septembre 2018, p. 474.

[757] C. const., Décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*, *JORF* n°0141 du 21 juin 2018 [en ligne].

[758] *Idem*, cons. 71.

[759] C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.*

[760] *Idem*, cons. 34.

[761] Transposant l'article 11 de la DPJ.

fondée exclusivement sur un algorithme dans deux cas[762]. En premier lieu, l'interdiction concerne toute décision ayant des effets juridiques défavorables pour la personne concernée. En deuxième lieu, l'interdiction porte sur toute décision affectant la personne concernée de manière significative. Il s'agit notamment d'interdire le recours à des décisions automatisées à des fins d'évaluation des aspects personnels ou de profilage pouvant conduire à une discrimination sur la base de données qualifiées comme sensibles au sens de la règlementation relative à la protection des DACP[763]. Dès lors, les exigences constitutionnelles concernant l'usage des SIA reposent exclusivement sur le traitement de DACP[764].

292. Cependant, le régime juridique actuel ne permet pas de répondre à toutes les interrogations concernant les algorithmes, notamment les SAAD. En ce sens, le Conseil d'État s'inquiétait des potentialités de voir apparaitre des « biais d'automatisation » par l'usage de SAAD. En d'autres termes, il redoutait de voir apparaitre une tendance consistant à « accorder aux analyses et aux recommandations de la machine une confiance excessive et, le cas échéant, supérieure à son propre jugement d'humain (voire à celui d'un tiers) »[765]. Ces biais, aussi appelés de « biais de confiance »[766], consistent à s'en remettre entièrement aux décisions fournies par le SAAD en ignorant tout autre voie possible. En ce sens, les lignes directrices relatives à la prise de décision automatisée du Comité européen de protection des données rappellent que « pour qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique. Le contrôle devrait être effectué par une personne qui a l'autorité et la compétence pour modifier la décision »[767].

---

[762] DPJ, art. 11 et LIL, art. 95.

[763] G29, « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 », 3 octobre 2017 (version révisée du 6 février 2018), p. 11 [en ligne] ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 350.

[764] Le juge constitutionnel effectue un contrôle de leur usage en vérifiant que le législateur à assurer la conciliation entre les objectifs d'intérêt général poursuivis et le droit au respect de la vie privée. À cette fin, les Sages doivent déterminer si le législateur a mis en œuvre des garanties suffisantes, dont principalement celles énoncées par la règlementation relative à la protection des DACP.

[765] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 350.

[766] CUMMINGS (M. L.), "Automation and accountability in decision support system interface design", *Journal of Technology Studies* n° 1, vol. 32, 2006.

[767] G29, « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 », *op. cit.*, p. 23.

293. L'absence de cadre juridique adapté aux usages des SAAD pose problème dans la mesure où l'usage de caméras « augmentées » par le secteur privé comme par le secteur public est en pleine expansion. Or, les caméras « augmentées » filmant la voie publique reposent précisément sur l'association de SAAD à des systèmes de vidéoprotection (fixes et aéroportés) à des fins d'analyse d'images. Dès lors, le recours à cette technologie nécessite un encadrement strict, explicite et adapté à chaque type de finalités[768]. De fait, l'emploi de cette technologie n'est régi que par quelques dispositions générales et décisions portant sur les algorithmes traitant des DACP qui s'avèrent, cependant, insuffisantes pour garantir l'exercice des droits et libertés face aux enjeux que présentent son usage dans le domaine pénal[769]. Aussi, en accord avec les recommandations formulées par les différentes institutions[770], l'usage expérimental à durée déterminée est privilégié et nécessite dès lors la mise en œuvre de dispositions juridiques provisoires pour la durée de l'expérimentation.

2. Un premier encadrement juridique expérimental des caméras « augmentées » de sécurité publique

294. Sous la pression des évènements sportifs à venir[771], le législateur a adopté des dispositions provisoires destinées à encadrer l'usage d'algorithmes « augmentés » équipant des caméras de vidéoprotection (fixes et aéroportées). La loi relative aux Jeux Olympiques et Paralympiques de 2024[772] (JOP2024) du 19 mai 2023 permet d'encadrer le déploiement - à titre expérimental - de caméras « augmentées » filmant la voie publique pour une période déterminée[773]. Elle comprend un chapitre III intitulé « Dispositions visant à mieux garantir la sécurité » dont

---

768 Sénat, Rapport d'information sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, pp. 84-85.

769 CNCDH, Avis IA, *op. cit.*, (6) p. 6 : « « Les réglementations en vigueur fournissent des références seulement partielles, qu'il s'agisse de la protection des données personnelles […] (RGPD) ou de la non-discrimination. Cela demeure insuffisant dès lors qu'un grand nombre de systèmes d'IA fonctionnent à partir de données non identifiantes et peuvent avoir des conséquences sur les droits fondamentaux excédant la protection des données personnelles et la non-discrimination ».

770 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 46-47 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

771 En témoigne la qualification de procédure accélérée du projet de loi.

772 Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *JORF* n°0116 du 20 mai 2023 [en ligne].

773 Celle-ci courant du début de la Coupe du monde de rugby ayant lieu en France à l'automne 2023 (à des fins de première expérimentation) jusqu'au 31 mars 2025 (date de finalisation des analyses et rapports de synthèse des expérimentations), selon l'article 10 de loi JOP 2024.

l'article 10 porte spécifiquement sur l'introduction législative de l'utilisation de caméras de vidéoprotection « augmentées » fixes et mobiles (incluant les caméras aéroportées) à titre expérimental. En d'autres termes, le texte autorise le recours à des caméras filmant l'espace public équipées d'algorithmes d'analyse d'évènements.

295. Ce texte s'inscrit dans le sens des recommandations formulées par la CNIL, dans sa position de juillet 2022, qui estimait que compte tenu des conséquences sur les droits et libertés qu'implique l'utilisation de caméras « augmentées » à des fins de police administrative comme de police judiciaire, leur encadrement relevait du domaine de la loi, en vertu de l'article 34 de la Constitution[774]. Ainsi, elle considère que le changement de paradigme institué par le recours à des algorithmes d'analyse en temps réel d'images de vidéoprotection conduisant à « une intervention immédiate ou [à] l'enclenchement de procédures administratives ou judiciaires par les services de police » nécessite la mise en œuvre d'un cadre légal spécifique[775]. En outre, il convient de souligner que le caractère même expérimental de ce recours n'ôte en rien la nécessité d'adopter des dispositions législatives adaptées compte tenu des modifications dans l'exercice des missions des forces de l'ordre qu'induisent l'utilisation des caméras « augmentées ». Dans un avis rendu le 12 octobre 2021, le Conseil d'État avait adopté une position similaire estimant que ces usages nécessitaient la mise en œuvre d'une législation spécifique[776]. Cet avis, non publié, avait été toutefois cité dans le rapport du Sénat publié en mai 2022[777] qui approuvait l'avis de la Haute juridiction, ajoutant qu'il en allait de la licéité de leur usage compte tenu du fait que ces dispositifs algorithmiques étaient développés par des acteurs privés[778].

---

774 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 15.

775 *Idem*.

776 CE, avis n°404020 du 12 octobre 2021 (non publié ; cité par CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, notes de bas de page pp. 15-16) : « les traitements des images issues de la vidéoprotection par le biais d'un logiciel d'intelligence artificielle, constituent des traitements de données personnelles distincts de ceux des images issues de la vidéoprotection et que ceux-ci […] sont susceptibles de porter une atteinte telle à la liberté individuelle qu'elles affecteraient des garanties fondamentales […] des libertés publiques au sens de l'article 34 de la Constitution du 4 octobre 1958 ».

777 Sénat, Rapport d'information sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*

778 *Idem*, p. 89.

296. Il est regrettable que la loi JOP2024, pourtant attendue, arrive aussi tardivement[779] compte tenu de la connaissance très en amont des grands évènements à venir et de l'utilisation prévue de longue date de technologies algorithmiques associées aux caméras de vidéoprotection[780]. Il convient de noter que suite aux avis rendus par la CNIL et par le Conseil d'État[781], une nouvelle version du texte JOP2024 avait été déposée par le Sénat le 22 décembre 2022 qui n'avait pas été réexaminée par les deux institutions[782]. Aussi, plusieurs organisations internationales s'étaient opposées à l'adoption des dispositions de la JOP2024 qu'elles jugeaient contraires aux dispositions internationales relatives aux droits de l'Homme[783]. Outre le renforcement des restrictions quant à l'exercice des droits et libertés, ces organisations estimaient que l'usage de ces technologies constituait bien un traitement de données biométriques au sens des textes européens[784]. Aussi, elles exprimaient leur regret de voir la France devenir un leader européen en matière de surveillance de l'espace public. Pourtant, en dépit des inquiétudes exprimées par les différents organismes défenseurs des droits et libertés, le Conseil constitutionnel a estimé, dans sa décision du 17 mai 2023[785], que les dispositions de la loi JOP2024 autorisant le recours à des caméras « augmentées »

---

779 CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, avis n° 22017438, p. 1 [en ligne] : « De manière générale, la Commission regrette d'avoir à se prononcer en urgence sur les évolutions envisagées par le projet de texte compte tenu de la prévisibilité, largement connue à l'avance, de l'évènement et des enjeux importants s'agissant de la vie privée des personnes concernées ».

780 L'appel à projets « Flash » (AAP) de 2019 portant sur « La Sécurité des Jeux Olympiques et Paralympiques de Paris 2024 reposait sur plusieurs thématiques pouvant inclure le recours à des algorithmes « augmentés » associés à des caméras de vidéoprotection à l'image de la thématique relative à la gestion des mouvements de foule sur laquelle portait le projet ANR GIRAFE qui s'est terminé en décembre 2021. Le législateur a ainsi manqué une opportunité de légiférer en amont une technologie qui pourtant reste sujet à controverses et méritait une réflexion plus approfondie.

781 CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 15 décembre 2022 [en ligne].

782 CNIL, « Jeux olympiques et paralympiques 2024 : la CNIL publie son avis sur le projet de loi », *cnil.fr*, 4 janvier 2023 [en ligne].

783 European Center for Not-for-profit Law (ECNL), « Lettre de la société civile sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », *ecnl.org*, 7 mars 2023 [en ligne] ; Human Rights Watch, « France : Rejeter la surveillance dans la loi sur les Jeux Olympiques 2024 - Un système de surveillance basé sur des algorithmes violerait les droits fondamentaux », *hrw.org*, 7 mars 2023 [en ligne] ; « Les mesures de vidéosurveillance algorithmique introduites par la loi JO 2024 sont contraires au droit international », *Le Monde*, 7 mars 2023 [en ligne] ; « 35 organisations internationales demandent le retrait de l'article 7 du projet de loi JO 2024 », *NextInpact*, 7 mars 2023 [en ligne] consultés le 27 mars 2023.

784 Human Rights Watch, « France : Rejeter la surveillance dans la loi sur les Jeux Olympiques 2024 - Un système de surveillance basé sur des algorithmes violerait les droits fondamentaux », *op. cit.* : Dès lors, elles considéraient qu'en toute logique des caméras « augmentées » filmant l'espace public visant à détecter des évènements suspects ou des comportements anormaux « capteront et analyseront forcément des traits physiologiques et des comportements de personnes présentes dans ces espaces » et que « le fait d'isoler des personnes par rapport à leur environnement, qui s'avère indispensable en vue de remplir l'objectif du système, constitue une "identification unique" ».

785 C. const., Décision n° 2023-850 DC, 17 mai 2023, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*, *JORF* n°0116 du 20 mai 2023 [en ligne].

de vidéoprotection afin d'encadrer les évènements à caractère sportif et festif des JOP de Paris 2024 étaient conformes à la Constitution[786].

297. Bien que le cadre législatif élaboré en vue de l'utilisation d'algorithmes « augmentés » équipant les systèmes de vidéoprotection soit nécessaire et salutaire, celui-ci n'est que temporaire puisqu'il vient répondre aux besoins d'une exploitation à titre expérimental de cette technologie et n'a donc pas nécessairement vocation à être pérennisé. En ce sens, la CNIL insistait sur le caractère expérimental de ces usages et que ceux-ci ne devraient « en aucun cas préjuger d'une éventuelle pérennisation de ces systèmes »[787]. S'étant pleinement saisie du sujet, la CNIL a d'ores et déjà entamé l'élaboration d'une doctrine d'emploi générale en matière d'IA ainsi que la publication de recommandations durant l'année 2023[788]. Néanmoins, la question du recours à des caméras de vidéoprotection « augmentées » devra faire l'objet d'un cadre juridique adéquat répondant aux différents enjeux qu'elles présentent et ce dans les plus brefs délais compte tenu de leur utilisation inévitable. Face aux enjeux que soulèvent les algorithmes « augmentés » associés aux caméras de vidéoprotection, la CNIL a pris la décision de l'inclure au sein de ses thématiques prioritaires pour 2023[789].

298. L'élaboration d'une législation pérenne applicable aux technologies « augmentées » nécessitera l'implication de différents acteurs : chercheurs issus des domaines pluridisciplinaires, industriels, utilisateurs au sein des forces de l'ordre et des services de secours mais aussi des autorités administratives indépendantes (AAI) telles que la CNIL, l'Agence nationale de sécurité des systèmes d'information (ANSSI), ou encore le Défenseur des droits. Aussi, l'efficacité d'une telle législation dépendra de l'intelligibilité de son contenu permettant de répondre aux enjeux présents et d'une formulation permettant de s'adapter aux évolutions du domaine afin d'anticiper les enjeux futurs (comme ce fut le cas lors de l'élaboration de la LIL).

---

[786] *Idem*, cons. 46 et 49.

[787] CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, *op. cit.*

[788] *Idem*.

[789] CNIL, « Thématiques prioritaires de contrôle 2023 : caméras « augmentées », applications mobiles, fichiers bancaires et dossiers patients », *cnil.fr*, 15 mars 2023 [en ligne]. Voir aussi : CNIL, Webinaire sur « Caméras "augmentées" dans les espaces publics », 23 mai 2023 [en ligne].

CONCLUSION DU TITRE I

299. Au vu de leurs nombreux atouts, les drones aériens « augmentés » de sécurité publique ont le potentiel requis afin de pallier les inconvénients auxquels sont sujets les autres caméras de vidéoprotection et d'accroitre l'efficacité des outils de surveillance de l'espace public. Aussi, il faut reconnaitre les efforts qui ont été entrepris afin d'établir un cadre juridique comprenant des mesures préventives d'utilisation de ces drones aériens face aux enjeux de sécurité publique s'agissant principalement de l'intégrité des personnes au sol ainsi que la sécurité des autres aéronefs évoluant au sein de l'espace aérien national. En outre, les autorités nationales et européennes ont pris la mesure des besoins en matière d'encadrement des technologies incluant des algorithmes d'IA et ont largement entamé leur processus d'élaboration de dispositions contraignantes à l'égard de leurs concepteurs et utilisateurs.

300. Néanmoins, l'existence d'un cadre juridique en matière de conception et de recours à de nouvelles technologies de surveillance de l'espace public ne suffit pas à l'établissement d'un lien de confiance entre les autorités publiques et les individus. La multiplication et la diversification des caméras de surveillance de l'espace public - enrichies de surcroit par des algorithmes d'analyse d'évènements - suscite des inquiétudes légitimes quant aux restrictions qu'elles génèrent pour l'exercice des droits et libertés.

301. Face aux enjeux que présentent les politiques sécuritaires et l'usage exponentiel des technologies numériques, le sociologue Zygmunt Bauman s'inquiétait de la banalisation de ces usages. Il craignait que la prise de conscience par la population générale des conséquences de cette utilisation arrive trop tardivement et que les moyens permettant de contrer ses effets aient disparu ou aient été vidé de leur substance[790]. Aussi, la loi RPSI tend à aller dans ce sens en laissant craindre un recours fréquent aux drones aériens par les forces de l'ordre, compte tenu de l'étendu du champ des finalités que lui a laissé le législateur.

[790] CHARDEL (P-A.) (dir.), *Politiques sécuritaires et surveillance numérique*, *op. cit.*, pp. 53-54.

TITRE II LE RENFORCEMENT DE LA SÉCURITÉ DANS LE RAPPORT SÛRETÉ-SÉCURITÉ INDUIT PAR LES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

302. Les drones aériens de sécurité publique, au même titre que les autres dispositifs de surveillance de la voie publique, constituent un nouvel outil de contrainte pour les droits et libertés. En outre, ils sont susceptibles de mettre ces droits et libertés en péril car comme tout objet connecté ils ne sont pas exempts de contenir des vulnérabilités exploitables par des attaques informatiques qui pourraient porter atteinte aux données qu'ils auront collectées. Aussi, le recours à des dispositifs vidéo associés à des algorithmes n'est pas un acte anodin, plus particulièrement lorsqu'il s'agit d'algorithmes « augmentés ». Le recours à des algorithmes dans le processus décisionnel des forces de l'ordre peut être sujet à des dérives pouvant porter de graves atteintes aux droits et libertés voire de contrevenir à leur exercice (**Chapitre 1**).

303. L'association d'algorithmes « augmentés » à des drones aériens dans un cadre de sécurité publique laisse craindre une accentuation du phénomène visant à privilégier la sécurité sur la sûreté. Le phénomène de « solutionnisme technologique », dénoncé par les défenseurs des droits et libertés, ne cesse de s'étendre au sein de la sphère régalienne et conduit à deux principaux constats en matière de sécurité publique. D'une part, les technologies « augmentées » à l'usage de la sécurité publique questionnent la souveraineté de l'État quant à ses missions de sauvegarde de l'ordre public relevant pourtant du domaine régalien. En cela, elles s'inscrivent dans un mouvement depuis longtemps observé consistant à promouvoir la participation du secteur privé à l'exercice des activités de sécurité et notamment de sécurisation de la voie publique. D'autre part, les technologies « augmentées » offrent l'illusion de fournir des solutions - en apparence - incontestables aux forces de l'ordre et aux services de secours. Aussi, leur utilisation à des fins préventives comme répressives interrogent les conséquences qu'elles peuvent avoir lorsqu'elles participent à l'établissement de preuves dans le cadre du procès pénal (**Chapitre 2**).

CHAPITRE 1 LES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE, VECTEURS DE LIMITATIONS DES DROITS ET LIBERTÉS

304. La forte opposition dont ont fait l'objet les drones aériens de vidéoprotection s'explique principalement par la crainte qu'ils suscitent d'accroitre le sentiment de surveillance généralisée des individus sur la voie publique. Il est vrai que le caractère d'outil « omniscient » qu'ils renvoient en raison de leur capacité à survoler les évènements, vient accentuer la perception d'une surveillance permanente de la population. L'acceptabilité juridique et sociétale des drones aériens de sécurité publique repose tant sur l'existence d'un encadrement strict de leur emploi (notamment s'agissant des données qu'ils sont en mesure de collecter) que sur la transparence de leur utilisation.

305. L'emploi de drones aériens « augmentés » renferme différents enjeux juridiques ayant une incidence directe ou indirecte sur les droits et libertés. Le recours croissant aux technologies telles que les drones aériens « augmentés » par les forces de sécurité publique vient renforcer les contraintes portées tant aux libertés individuelles[791], telles que le droit à la protection du droit à la vie privée et des données à caractère personnel, qu'aux libertés collectives, comme le droit de manifestation. Aussi, le recours aux technologies numériques comprend invariablement des risques pour la sécurité des objets connectés et des données qu'ils collectent. Toute technologie numérique est, de fait, susceptible de comporter des vulnérabilités conduisant à une perte de leur contrôle ou à des atteintes aux données collectées (**Section 1**).

306. Aujourd'hui, le recours à des drones aériens à des fins de sécurité publique dépasse les enjeux induits par la collecte de données et inclut ceux liés à l'analyse de celles-ci par des SIA. Ce qui autrefois relevait du fantasme est désormais réalité comme en témoigne la loi JOP2024 autorisant l'expérimentation de caméras de vidéoprotection associées à des algorithmes d'analyse d'évènements. Le dernier Livre blanc sur la sécurité intérieure évoquait cette volonté des pouvoirs publics d'exploiter les algorithmes « augmentées » afin d'améliorer l'encadrement des grands évènements et n'exclut pas leur recours à des fins de police judiciaire. Cependant, les technologies algorithmiques ne sont pas exemptes de défauts tant dans leur conception que dans leur utilisation et

[791] MASSET (C.), « Gendarmerie du transport aérien : réglementation de l'utilisation des drones aériens », pp. 168 et 172 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

peuvent porter une atteinte directe aux droits et libertés (**Section 2**).

Section 1 Un renforcement des limitations des droits et libertés par les drones aériens « augmentés » de sécurité publique

307. L'accroissement des usages technologiques au sein des activités de sécurité publique engendre un bouleversement dans le rapport sûreté-sécurité en renforçant les contraintes imposées aux droits et libertés au profit de mesures visant à prévenir les atteintes à l'ordre public et aider à la recherche des auteurs d'infractions. Ces technologies collectent un grand nombre de données dont principalement celles relatives aux individus. En ce sens, les technologies issues de la vidéoprotection ont largement contribué au processus de massification et de diversification des données pouvant être collectées sur les individus. Le traitement massif de DACP par les forces de l'ordre, même lorsqu'il est effectué dans un cadre légal, n'en est pas moins extrêmement intrusif avec des conséquences non négligeables sur le comportement des individus. La banalisation des usages de la vidéoprotection (principalement des caméras fixes filmant la voie publique) aura ainsi permis d'étendre son champ à d'autres outils filmant la voie publique dont l'action vient amplifier les enjeux juridiques initiaux.

308. Les drones aériens sont par nature des objets dont l'objectif principal repose sur la collecte de données[792]. Dans un cadre de sécurité publique, les drones aériens partagent inévitablement des enjeux juridiques similaires à ceux des autres outils de vidéoprotection. Toutefois, ils offrent une vision de ces enjeux quelque peu différente par leur caractère aérien, mobile et miniaturisé. Ils présentent une opportunité pour les forces de l'ordre et les services de secours de collecter davantage de données liées ou non à des individus pouvant ainsi aggraver le phénomène de massification de la collecte observée avec d'autres technologies de surveillance. Néanmoins, ils disposent d'un cadre d'utilisation différent de ces autres technologies de surveillance du fait qu'ils ne sont pas employés de manière permanente (comme le serait une caméra fixe). Cette particularité fait qu'ils sont susceptibles de collecter des données de manière plus ciblée, permettant d'espérer une modération de leur incidence sur les droits et libertés. Pour autant, les drones aériens de sécurité publique modifient le regard qu'il convient de porter au type et

[792] STORR (P.) and STORR (C.), « The Rise and Regulation of Drones : Are We Embracing Minority Report or WALL-E ? », p. 106 *in* CORRALES (M.), FENWICK (M.) and FORGÓ (N.) (Ed.), *Robotics, AI and the Future of Law*, *op. cit.*

à la quantité de données collectées. Leur taille et leur caractère aérien nécessitent l'adoption d'une nouvelle approche de la collecte des données dans les activités de sécurité publique. Cette expansion de la collecte de données par les drones aériens de sécurité publique met en lumière la pérennisation d'un état d'exception reposant sur une surveillance constante qui répondrait au besoin de sécurité exprimé par les individus, tout en restreignant leurs droits et libertés (§1).

309. Aussi, la numérisation des activités des forces de l'ordre et des services de secours doit également faire face aux enjeux majeurs que présentent la sécurité des systèmes d'information et des objets connectés. Les forces de l'ordre et les services de secours ne sont pas à l'abri d'une attaque informatique ou même d'une usurpation du contrôle d'un objet connecté ou de tout autre technologie issue de leur arsenal. En ce sens, l'introduction des drones de sécurité publique au sein de l'espace aérien national comporte inévitablement des enjeux en matière de sécurité des outils et des données numériques issus des activités de sécurité publique (§2).

§1. L'amplification de la surveillance de masse par les drones aériens « augmentés » de sécurité publique

310. La vidéoprotection étant toujours plus présente au quotidien, il semble opportun d'aborder ses effets tant sur le comportement des individus que du point de vue de l'exercice de leurs droits et libertés. En ce sens, l'emploi de caméras de surveillance présente plusieurs atouts néanmoins contrecarrés d'enjeux en termes d'incidences sur les droits et libertés. L'ancrage des systèmes de vidéoprotection dans l'espace public est un témoin de la priorité octroyée aux moyens de sécurité au détriment des droits et libertés, qu'ils soient individuels ou collectifs. Parmi ces droits et libertés individuels, la liberté personnelle[793] permet « un certain secret des déplacements des personnes qui utilisent leur liberté d'aller et venir »[794] et recouvre le droit au respect de la vie privée. Dès lors, le développement exponentiel du réseau de caméras de surveillance de la voie publique a indubitablement conduit à une disparition progressive de cet anonymat en offrant la possibilité aux forces de l'ordre de suivre les déplacements et les interactions entre les individus au

[793] La liberté personnelle est apparue dans la jurisprudence du Conseil constitutionnel dès les années 1980 (C. const., Décision n°88-244 DC, 20 juillet 1988, *Loi portant amnistie*, cons. 22 [en ligne] et C. const., Décision n° 89-257 DC, 25 juillet 1989, *Loi modifiant le code du travail et relative à la prévention du licenciement économique et au droit à la conversion*, cons. 23 [en ligne]). Elle est constitutionnellement reconnue et rattachée aux articles 2 et 4 de la DDHC (C. const., Décision n° 2003-484, 20 novembre 2003, *Loi relative à la maitrise de l'immigration, au séjour des étrangers en France et à la nationalité*, *JORF* n°274 du 27 novembre 2003, cons. 94 [en ligne]).

[794] OBERDORFF (H.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 404.

sein de l'espace public. Ainsi, les drones aériens de sécurité publique devraient inévitablement accentuer l'incidence des technologies de surveillance de la voie publique sur les droits et libertés (A).

311. Les enjeux juridiques entourant les caméras de surveillance reposent essentiellement sur une collecte et un traitement massif de données dont certaines sont reconnues comme étant des DACP. Or, la collecte de ces données n'est pas anodine, particulièrement dans un cadre régalien où elles font l'objet d'une protection spécifique au niveau national et supranational. Ainsi, les données collectées par les caméras de surveillance, lorsqu'elles permettent de reconnaître ou d'identifier (y compris par individualisation ou par corrélation des données[795]) une personne, seront qualifiées de DACP et constituent par conséquent une intrusion dans la vie privée au sens de la jurisprudence[796] et des textes en matière de protection des données. Néanmoins, la LIL permet, encore aujourd'hui, d'encadrer la création de fichiers et la mise en œuvre de traitements de DACP. En outre, elle autorise la création de fichiers de traitements automatisés de DACP à des fins policières sous réserve que ceux-ci soient en accord avec certains principes généraux[797] et assurent l'exercice des droits des individus. La multiplication du nombre des fichiers de police demeure ainsi une préoccupation essentielle des défenseurs des droits et libertés. Aussi, le législateur a progressivement augmenté les motifs permettant le fichage à des fins de sécurité, engendrant *de facto* de nombreux enjeux tenant autant à la gestion des données qu'au contrôle de leur traitement (B).

A. Les effets de l'amplification de la surveillance de masse

312. Le premier enjeu engendré par le recours à des drones de sécurité publique est aisément identifiable car il reproduit et amplifie un phénomène depuis longtemps observé par l'utilisation d'autres outils de vidéoprotection, celui d'une surveillance de masse. Les effets de la surveillance des personnes sur la voie et dans les lieux publics devraient inévitablement être décuplés par l'arrivée des drones aériens, dont les capacités dépassent largement celles d'autres systèmes de

[795] Voir en ce sens : G29, Avis 05/2014 sur les Techniques d'anonymisation, *op. cit.*, pp. 12-13 ; CNIL, « Identifier les données personnelles », *op. cit.*

[796] Voir en ce sens : C. cass., 1ère ch. civ., 21 mars 2006, n°05-16.817 [en ligne] ; CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, n° 44647/98, § 57 [en ligne].

[797] Principe de licéité et de loyauté des informations collectées et conservées, principe de finalité quant à l'utilisation ultérieure d'un fichier, principe d'exactitude des informations conservées, droit à l'information ou encore droit d'accès des personnes concernées aux DACP les concernant.

vidéoprotection. Cette technologie dispose d'atouts qui lui permettent d'accéder à des lieux et d'offrir des points de vue dont ne disposaient pas les agents des forces de l'ordre et des services de secours auparavant. En outre, leur petite taille offre des potentialités d'observation et principalement de discrétion inégalables par d'autres formes de caméras de surveillance.

313. Les effets induits par la surveillance de masse supposent que plus les personnes font l'objet d'une observation plus la sphère de leur vie privée diminue[798]. Cette « sphère privée » reflète l'intimité de la personne et peut s'exprimer autant dans l'espace privé que dans l'espace public. Il semble périlleux de vouloir définir juridiquement la notion de vie privée tant il est difficile d'en délimiter précisément les contours[799]. Néanmoins, cette notion devrait être comprise comme une nécessité propre à l'être humain sans laquelle il ne peut exister. Les professeurs Xavier Latour et Bertrand Pauvert offrent une ébauche de définition de la notion de vie privée comme le besoin pour « toute personne à […] une sphère d'intimité, inviolable, qui n'appartienne qu'à elle et dont elle ne doit rendre compte à quiconque »[800]. Un rapport d'information au Sénat portant sur la relation entre vie privée et outils numériques énonce que le droit au respect de la vie privée renferme les concepts tant d'intimité que d'autonomie[801] et peut être compris comme « un droit à la tranquillité »[802].

314. La protection et le respect de la vie privée repose ainsi sur une liberté de choix d'un individu sur sa vie privée. En d'autres termes, la faculté de chaque individu « de déterminer librement sa vie privée est la manifestation même de l'existence d'une sphère privée soustraite aux ingérences étatiques »[803]. *De facto*, les choix tant affectifs que sentimentaux de chaque individu ne peuvent faire l'objet d'aucune immixtion extérieure. En ce sens, une décision de la Cour d'appel de Paris énonce que le respect du droit à la vie privée constitue « le droit pour une personne d'être libre

---

[798] DELFORGE (A.) et GÉRARD (L.), « Chapitre 1. - Les robots : source de risques pour la vie privée ? », p. 145 *in* DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, Bruxelles, éd. Larcier, 2017, 482 p.

[799] En ce sens, le professeur Robert Badinter avait affirmé que « s'agissant de la vie privée, [...] plutôt que de définir le contenu, les juristes français se sont plus volontiers attachés à dépeindre le contenant […] mais quant au domaine qu'il enclôt, ses dimensions s'avèrent singulièrement variables » (BADINTER (R.), « Le droit au respect de la vie privée », *JCP G* 1968, I, 2136).

[800] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 182.

[801] Sénat, Rapport d'information n° 441 (2008-2009) « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information » remis au nom de la commission des lois par DÉTRAIGNE (Y.) et ESCOFFIER (A-M.), 27 mai 2009 [en ligne].

[802] CARBONNIER (J.), *Droit civil*, vol. 1, Paris, PUF, 2004, 2574 p., p. 518.

[803] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, n°456, p. 741.

de mener sa propre existence comme elle l'entend avec un minimum d'ingérences de l'extérieur »[804]. En outre, la vie privée comprend plusieurs éléments tous liés aux droits de la personnalité qui peuvent être définis comme des « droits attachés à la personne elle-même, qui ont pour objet le respect de la personne dans ce qu'elle est »[805].

315. Enfin, le principe du respect de la vie privée induit le fait qu'une personne puisse conserver des secrets intéressant sa personne, en d'autres termes une forme de droit à l'anonymat qui ne pourra laisser la possibilité à aucun tiers de l'entraver. À ce titre, le droit au secret fait l'objet d'une protection judiciaire en tant qu'élément relevant du droit à la vie privée et comprend le secret de la correspondance. Bien qu'ayant été reconnu comme étant un principe à valeur constitutionnelle par le Conseil constitutionnel dans sa décision du 18 janvier 1995[806] qui le rattache à l'article 2 de la DDHC[807], le droit à la vie privée subit de multiples atteintes et restrictions par l'usage des technologies de surveillance telles que les systèmes de vidéoprotection. Ces technologies de surveillance sont ainsi autant porteuses d'opportunités d'amélioration de la sécurité publique qu'elles instaurent un mouvement général restrictif des droits et libertés. En cela, les drones de sécurité publique, par l'augmentation des possibilités de collecte de données couplée à leurs capacités de mobilité créent un effet d'amplification de la surveillance (1).

316. Aussi, l'accroissement des effets de la surveillance de l'espace public ne se limite pas à la seule collecte des DACP et tend à avoir des conséquences plus globales sur le comportement des individus, c'est à dire sur leur liberté d'agir et le choix du comportement qu'ils adoptent dans l'exercice de leur vie privée. En ce sens, Roger Clarke identifie plusieurs dimensions de la vie privée pouvant faire l'objet d'une atteinte par les drones aériens utilisés à des fins de surveillance

---

804 CA de Paris, 7ème chambre, 15 mai 1970.

805 BERTRAND-MIRKOVIC (A.), *Droit civil - personnes, famille*, Paris, éditions Studyrama, 4e édition, 2014, 495 p.

806 C. const., Décision n°94-352 DC, 18 janvier 1995, *op. cit.* et C. const., Décision n°2008-562 DC, 21 février 2008, *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*, *JORF* n°0048 du 26 février 2008 [en ligne].

807 C. const., Décision n°2012-652 DC, 22 mars 2012 *concernant la loi relative à la protection de l'identité*, *JORF* du 28 mars 2012 [en ligne]. : « la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen implique le droit au respect de la vie privée : que, par la suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ».

par les forces de l'ordre[808] : les DACP, l'intégrité du corps d'un individu[809], la liberté d'action et de comportement (*behavioural privacy*), ainsi que les habitudes ou expériences personnelles (2).

1. L'incidence sur les droits et libertés

317. Les drones aériens de sécurité publique présentent un large spectre d'atteintes potentielles aux droits et libertés à commencer par le droit au respect de la vie privée. En premier lieu, ils étendent le champ spatial de la surveillance de l'espace public par leur facilité de déploiement et leur capacité à traiter des données, notamment des images de personnes dans des endroits plus nombreux. En deuxième lieu, ils viennent intensifier les effets de la surveillance de l'espace public. Les individus circulant sur la voie publique pourront faire l'objet d'une observation de manière continue durant un évènement, avec des plans plus rapprochés et une haute résolution d'images. L'amélioration des conditions de captation des images et les possibilités de visualisation en temps réel des évènements en continu qu'offrent les drones aériens aux forces de l'ordre renforce le caractère intrusif des systèmes de vidéoprotection. Dès lors, ce n'est plus seulement le droit au respect de la vie privée qui est mis en péril mais aussi la liberté d'aller et venir. Celle-ci lui est étroitement liée puisqu'elle suppose également le respect de l'anonymat des personnes dans leurs déplacements[810]. L'intensification de la surveillance de l'espace public induit, en outre, une augmentation du nombre d'images collectées par les drones aériens de sécurité publique, qui renforce les enjeux tenant aux conditions de conservation et de réutilisation des données collectées.

---

[808] CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, spéc. pp. 287-288.

[809] Il convient de remarquer que cette dimension a été relevée sous l'angle du droit anglo-saxon. En droit français, l'intégrité physique des personnes ne relève pas du droit à la vie privée mais du droit à la vie tel qu'énoncé par l'article 2 de la Conv.EDH (OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit*., p. 576 ; ROUVILLOIS (F.), *Libertés fondamentales*, Paris, Flammarion, coll. Champs-Université, 2ème édition, 2016, 446 p., p. 233) et est également protégé par l'article 16-3 du Code civil (CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit*., pp. 497-502). Aussi, cette dimension ne semble plus véritablement pertinente compte tenu des règles techniques et juridiques mises en œuvre en matière de navigabilité.

[810] CNIL, 24ème Rapport d'activité de 2003, *op. cit.*, p. 135 : « L'anonymat est en effet une condition nécessaire de la liberté d'aller et venir ou de la préservation de la vie privée ». Voir aussi : OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 404 : La vidéoprotection engendre des atteintes aux libertés individuelles qui garantissent « un certain secret des déplacements des personnes qui utilisent leur liberté d'aller et venir » ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 9 : Face au déploiement des caméras de vidéoprotection « augmentées », « la préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice » des libertés individuelles comme le droit à la vie privée et la liberté d'aller et venir qui s'exercent dans des espaces publics ; OBERDORFF (H.), « La liberté individuelle face aux risques des technologies de sécurité », *in* ROBERT (X.), *Mélanges Jacques Robert. Libertés*, Paris, Montchrestien, 1998, 608 p., p. 177 ; HANICOTTE (R.), « Espace public, impasse des libertés », *op. cit.*

318. Le recours à des drones aériens à des fins de surveillance de l'espace public engendre un double effet d'amélioration du suivi d'individus. Il induit un effet positif au regard des besoins des forces de l'ordre et des services de secours qui ne seront plus limités par les obstacles obstruant leur visibilité et bénéficieront d'angles de vue qu'aucun autre type de caméra ne serait capable de produire. Aussi, la captation d'images en continu offre de meilleures conditions de suivi d'individus (*tracking*) et par conséquent de poursuite des auteurs d'infractions. Néanmoins, cet effet suscite en contrepartie un effet négatif d'influence du comportement des individus et de surveillance accrue (aussi appelé effet « paparazzi »[811]). Les drones aériens de sécurité publique pourraient ainsi être à l'origine de modifications du comportement en réaction à leur présence. Les individus se sentant observés chercheraient alors à éviter de se trouver dans le champ d'observation du drone aérien afin de préserver leur sphère privée. Cependant, cette influence sur le comportement des individus pourrait *a contrario* être interprétée comme une forme de comportement caractérisé d' « anormal » ou faire l'objet d'une interprétation erronée par les agents observateurs.

319. En dépit des nombreuses qualités que présentent les drones aériens, certaines de leurs capacités pourraient aussi présenter des défauts. Le caractère mobile des drones aériens leur donne la possibilité de capter des images au plus près des évènements. Cependant, cette qualité pourrait aussi être un défaut en limitant le contexte d'interprétation des évènements qui ne présenterait qu'un angle de vue du déroulement de l'action. Cette proximité des évènements serait donc aussi susceptible d'amener les agents à formuler de fausses conclusions et de les induire en erreur dans leur interprétation des évènements (ex. erreur sur l'individu véritablement à l'origine d'un trouble à l'ordre public, interprétation erronée des agissements due à un manque d'informations, etc.). Ces erreurs sont dès lors susceptibles de porter atteinte à plusieurs droits et libertés, notamment au droit à la sûreté. À l'instar d'autres caméras de vidéoprotection, il s'avèrera difficile de contester les accusations devant l'opinion publique, voire dans le cadre d'un procès pénal[812], qui reposeront sur les images captées par les drones aériens, notamment du fait des limites portées au droit d'accès en matière de sécurité publique.

320. Ces nouvelles technologies présentent en outre un défaut similaire : celui d'une distanciation avec la réalité aussi désignée sous les termes anglo-saxon de *Moral Buffer*[813]. Les

[811] CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 289.

[812] *Idem*, p. 290.

[813] CUMMINGS (M. L.), "Automation and accountability in decision support system interface design", *op. cit.*

agents qui piloteront les drones aériens ne sont pas ceux chargés d'observer en temps réel les images qu'ils capteront. De même que pour les opérateurs chargés de visualiser les images issues des caméras fixes de vidéoprotection, les agents situés au centre de commandement qui observent l'afflux d'images transmises par les drones aériens agissent dans une forme de réalité virtuelle. Ce détachement vis à vis de la réalité, en comparaison des agents se trouvant sur les lieux, pourrait avoir une influence dans le processus décisionnel des agents, qui ne seraient soumis que dans une moindre mesure à des contraintes de conscience dans l'analyse des évènements. En d'autres termes, l'agent à distance peut être sujet au phénomène de distanciation morale par rapport aux événements. Cet éloignement peut engendrer un double effet. Un effet positif où l'agent-opérateur visionnant les images du fait de son éloignement du terrain sera moins enclin à analyser les évènements et à prendre des décisions sous l'effet des émotions[814]. À l'inverse, un effet négatif pourrait être que l'agent-opérateur prenne des décisions disproportionnées ou inadaptées par rapport à la situation en cours.

321. La miniaturisation des drones aériens leur offre une indéniable capacité de discrétion qui les distinguent des autres caméras de vidéoprotection. Ces drones aériens peuvent ainsi être conçus afin qu'ils ne puissent ni être vus ni même entendus. Néanmoins, cet atout peut induire une forme de surveillance dissimulée. En conséquence, la présence de ces caméras pourrait passer inaperçue au regard des personnes observées qui n'auraient alors pas conscience du fait même qu'elles sont surveillées et que des données les concernant font l'objet d'un traitement. Aussi, le pouvoir de discrétion des drones aériens s'accompagne d'un important enjeu de transparence quant aux critères sur lesquels reposera l'analyse du comportement des individus. Pour rappel, le législateur a mis en œuvre certaines garanties permettant aux personnes d'avoir connaissance du traitement de leurs données par les systèmes de vidéoprotection. La présence d'un drone à l'usage des forces de l'ordre doit par conséquent faire l'objet d'une information auprès du public par tout moyen[815].

322. Aussi, en vertu de la règlementation relative à la protection des DACP, toute personne dispose de droits à l'information, d'accès, d'opposition et de rectification sur ses données[816]. Le droit à l'information suppose que chaque personne a le droit de savoir quelles données la

---

[814] TESSIER (C.), « Autonomie : enjeux techniques et perspectives », p. 73 *in* DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*

[815] CSI, art. L242-3.

[816] RGPD, art. 13 à 16 et 21 ; DPJ, art. 13, 14, 16, 17 ; LIL, art. 48 à 50 et 116 à 118.

concernant a fait l'objet d'un traitement, la finalité de ce traitement et la personne qui en est responsable. Comme tout traitement de DACP, les enregistrements issus des drones aériens de vidéoprotection qui comportent des DACP sont soumis à la règlementation relative à leur protection[817]. Par conséquent, toute personne devrait pouvoir avoir accès aux enregistrements la concernant issus d'un drone aérien de sécurité publique, au même titre que dans le cas d'enregistrements issus de caméras fixes. Cependant, les enregistrements des drones aériens ne sont conservés que sept jours hormis les cas où ils donneraient lieu à l'ouverture d'une procédure judiciaire[818] ; en pratique il s'avèrera donc difficile de faire appliquer son droit d'accès. Aussi, bien que la législation exige des autorités publiques de respecter un devoir d'information du public de l'usage de drones aériens, les conditions d'utilisation et les qualités propres à cette technologie ne facilitent pas l'application concrète du principe, pourtant essentiel, qu'est celui de la transparence des usages technologiques.

2. L'incidence sur le comportement des individus filmés

323. La surveillance visible a une influence significative sur le comportement des individus et tend principalement à dissuader les agissements présentant un caractère illégal. À l'inverse, la surveillance dissimulée présente des effets globalement néfastes en induisant chez les individus la peur d'être observés à tout moment et que leur comportement puisse être perçu comme indésirable au point de faire l'objet d'une sanction. Les effets d'une surveillance dissimulée pourraient être qu'une personne qui appréhenderait d'être observée modifie son comportement. Les conséquences seraient alors qu'elle pratique une autocensure de ses agissements au sein de l'espace public. Ces effets conduiraient à une forme « d'autodiscipline » des personnes ou *a minima* d'un effet dissuasif sur de nombreux comportements aboutissant à une forme de gel de l'expression de leurs libertés et de leur créativité[819]. Aussi, certains aspects du comportement sont reconnus comme étant particulièrement sensibles au sentiment d'observation tels que la sexualité, les croyances religieuses ou encore l'adhérence à un parti politique[820]. L'amplification du sentiment d'observation pourrait conduire à des effets dévastateurs pour la vie de certaines personnes en créant une forme

[817] CSI, art. L. 242-4.

[818] *Idem*.

[819] CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 287.

[820] *Ibid*. Voir aussi : CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 60 ; FINN (R.) *et al.*, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations", *Publications Office of the European Union*, 2014. 38 p., p. 16 [en ligne].

d'isolement ou encore en obérant leurs capacités de créativité.

324. Ainsi, l'enjeu de cette surveillance va au-delà de la simple diminution de la sphère privée et tient dans les effets de la connaissance de cette surveillance par les individus. La perception et le sentiment de surveillance pourraient avoir des retombées sur les agissements des individus leur ôtant par voie de conséquence une certaine forme de liberté d'expression de soi (aussi appelée *behavioural privacy*). Certains auteurs évoquent la notion d' « effet dissuasif »[821] (*chilling effect*[822]) qui décrit la théorie selon laquelle « la seule connaissance de l'utilisation ou de la potentielle utilisation d'une technologie de surveillance va mener le citoyen à modifier son comportement »[823] et par conséquent à adopter un comportement d'« auto-censure »[824]. En d'autres termes, ce sont les activités personnelles, la liberté de mouvement, les centres d'intérêts et les préférences d'un individu qui pourraient être influencés par le sentiment de surveillance. Certains auteurs affirment même « qu'au-delà d'une surveillance réelle, la simple impression - voire la simple suspicion - quant à la possibilité de faire l'objet d'une écoute ou d'un enregistrement peut suffire à provoquer une forme de retenue de la part des personnes. Cette retenue peut s'interpréter comme une forme de renonciation ténue mais bien réelle au plein et entier exercice de son droit à la vie privée »[825].

325. L'enjeu induit par l'introduction des drones aériens de sécurité publique dépasse celui de la simple surveillance pour tendre vers celui du sentiment de surveillance, qu'il soit réel, supposé ou fictif, renforçant le risque d'atteinte au droit au respect de la vie privée. En d'autres termes, l'introduction des drones aériens au sein de l'espace public vient concrétiser une forme de

---

821 Le Conseil de l'Europe a définie la notion d' « effet dissuasif » comme « le fait de créer des inhibitions ou de décourager l'exercice légitime d'un droit » (CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 11).

822 Le terme anglo-saxon *chilling* signifiant « effrayant » ou « dissuasif », il est possible de traduire cette expression par « effet dissuasif » voire « effet paralysant ». Voir notamment : CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 287 ; STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit.*, p. 35.

823 Sénat, Rapport d'information sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 56. Voir aussi : CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, spéc. p. 99 ; EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », Version 2.0, 29 janvier 2020, 35 p., p. 5 [en ligne] ; STABEN (J.), « Der Abschreckungseffekt auf die Grundrechtsausübung : Strukturen eines verfassungsrechtlichen Arguments », *Mohr Siebeck*, 2016.

824 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 15.

825 DELFORGE (A.) et GÉRARD (L.), « Chapitre 1. - Les robots : source de risques pour la vie privée ? », p. 146 *in* DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, *op. cit.*

surveillance « permanente dans ses effets, même si discontinue dans son action »[826] entrainant des restrictions toujours plus importantes de l'exercice des droits et libertés.

326. La recherche par chaque individu d'un « espace privé » (ou d'un lieu d'intimité) s'exprime aussi bien dans les lieux privés que, d'une manière raisonnable, au sein des lieux publics. Cependant, les progrès technologiques présentent l'inconvénient d'accroitre considérablement les possibilités pour des tiers d'envahir cet « espace privé ». Or, les autorités publiques, en partenariat avec les entreprises spécialisées dans le secteur des hautes technologies, ont progressivement développé une tendance venant légitimer le recours systématique aux nouvelles technologies qui reposent sur un traitement massif de données. Le phénomène du « solutionnisme technologique » conduit alors inévitablement vers une destruction de cet « espace privé » au motif de vouloir renforcer la sécurité publique. L'argument qui tend à faire prévaloir la sécurité au détriment des libertés individuelles suscite légitimement l'inquiétude de voir les progrès technologiques vider peu à peu ces libertés de leur substance. Pourtant, le besoin irrépressible des êtres humains d'avoir un « espace privé » devrait bénéficier de garanties effectives. Ce besoin vital ne devrait pas dépendre du bon vouloir des autorités publiques. Les progrès technologiques ne doivent pas servir à renforcer les contraintes portées aux attentes légitimes des individus à un « espace privé »[827].

327. Indépendamment de la nécessité d'appliquer un principe de transparence, l'utilisation de drones aériens par les autorités publiques engendrent un renforcement de l'accoutumance des individus aux outils de surveillance[828]. Les qualités de mobilité et de miniaturisation des drones aériens leur confèrent l'avantage - et l'inconvénient - de pouvoir aisément échapper à la connaissance des personnes concernées déjà acclimatées à la présence d'outils de surveillance de la voie publique. En conséquence, les personnes observées pourraient s'habituer à la présence fréquente de drones aériens au sein de l'espace public. Cette capacité qu'ont les drones aériens, et de manière plus générale les outils numériques, de se fondre dans l'environnement du quotidien est

---

826 FOUCAULT (M.), *Surveiller et punir*, Paris, Gallimard, 1975, 318 p.

827 CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 288.

828 EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », *op. cit.*, p. 6 : « La surveillance systématique et automatisée d'un espace spécifique par des moyens optiques ou audiovisuels […] est devenue un phénomène important de notre époque ». Voir aussi : CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, pp. 47-67 ; DELFORGE (A.) et GÉRARD (L.), « Chapitre 1. - Les robots : source de risques pour la vie privée ? » *in* DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, *op. cit.*, spéc. p. 127 ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, spéc. pp. 139-140 ; CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.* ; STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit.*

précisément l'enjeu sur lequel repose la régression du droit à la protection de la vie privée. Ils ne sont, par ailleurs, pas toujours perçus comme des outils de collecte de DACP[829]. Cette présence quotidienne des technologies de surveillance permet pourtant une collecte massive de données de manière presque invisible aux yeux des individus, induisant un effet de surveillance passive et permanente.

B. Une expansion du traitement des DACP par les drones aériens « augmentés » de sécurité publique

328. L'enjeu lié à la collecte massive de données par les drones aériens « augmentés » de sécurité publique repose sur l'étendue du type de données qu'ils sont en mesure de collecter. De fait, ils sont susceptibles de collecter différents types de données (à caractère personnel et non personnel) lors des missions. Le fait est que les multiples capteurs qui équipent ces drones aériens couplés à leur mobilité leur permettent d'acquérir une plus grande quantité de données que tout autre système de vidéoprotection. Ils sont munis de caméras (œuvrant au pilotage du drone ainsi qu'à la captation d'images de la voie publique) mais aussi d'émetteurs-récepteurs GPS permettant la géolocalisation du drone aérien mais aussi potentiellement celles des individus observés. Or, ces opportunités de suivis d'individus sont attentatoires à la liberté personnelle et ne sont par conséquent autorisées que dans le cadre de la sauvegarde de l'ordre public[830]. Aussi, d'autres données relatives aux individus ou à des biens se trouvant sur les lieux peuvent également être collectées et analysées par les algorithmes « augmentés » (1). Aussi, l'importante quantité de données que peuvent collecter les drones aériens « augmentés » de sécurité publique pourraient éventuellement servir à enrichir le contenu des fichiers de police dans le cas où une procédure aurait été ouverte (2).

1. Une massification de la collecte de DACP

329. L'extension de la collecte de données, par l'intermédiaire de nouveaux dispositifs tels que les drones aériens, engendre des potentialités d'atteintes au droit à la protection des DACP. La

---

[829] DELFORGE (A.) et GÉRARD (L.), « Chapitre 1. - Les robots : source de risques pour la vie privée ? », p. 149 *in* DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, *op. cit.*

[830] CEDH, 6 septembre 1978, *Klass c. Allemagne*, n° 5029/71 [en ligne] : « le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques ». Cette décision s'avère capitale en ce qu'elle témoigne de la longévité d'une forme d'accoutumance à la généralisation de la surveillance policière.

massification de la collecte de données suscite des enjeux quant aux modalités de stockage ainsi qu'aux conditions d'accès assurant une confidentialité de ces données. Aussi, le principe de minimisation (autrefois intitulé « principe de proportionnalité ») énoncé par la règlementation sur la protection des données est atténué s'agissant de la DPJ en ce qu'il n'exige qu'un traitement non excessif des DACP[831]. Cette différence dénote une plus grande marge de manœuvre laissée au responsable de traitement dans le cadre des activités relatives au domaine pénal, qui laisse apparaitre un doute quant à la délimitation et la compatibilité des DACP collectées avec l'objet du traitement[832]. Ayant pris la mesure de cette difficulté lors de l'élaboration de la loi RPSI, le législateur conditionne la collecte de DACP par des drones aériens de sécurité publique à celles strictement nécessaires aux besoins de la mission[833], appliquant ainsi une version plus stricte du principe de minimisation à l'image de celui du RGPD[834].

330. Néanmoins, cette loi n'interdit que la captation du son et les traitements de reconnaissance faciale[835]. En outre, elle laisse le soin au préfet territorialement compétent de définir les données pouvant faire l'objet d'un traitement dans le cadre de chaque autorisation de recours à des drones aériens par les autorités publiques[836]. Dès lors, il faut espérer que ce dernier fera preuve de vigilance quant aux limites à porter au traitement de DACP. Aussi, la question du traitement des données définies comme sensibles au sens de la règlementation relative à la protection des DACP[837] vient renforcer les potentialités d'atteinte au droit à la protection de la vie privée et à leurs données. Bien que le législateur et le Conseil constitutionnel aient formellement interdit le recours à des

---

831 DPJ, art. 4. c). : Les DACP doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ».

832 PEYROU (S.), « La Directive 2016/680 du 27 avril 2016 (protection des données dans les domaines de la coopération policière et judiciaire en matière pénale) », *in* CHEVALLIER-GOVERS (C.) (dir.), *L'échange de données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*, Mare & Martin, 2017, 545 p., p. 479.

833 CSI, art. L. 242-4, al. 1er : la RPSI exige que « la mise en œuvre des traitements [de DACP] soit être strictement nécessaire à l'exercice des missions concernées et adaptée au regard des circonstances de chaque intervention » et qu' « elle ne peut donner lieu à la collecte et au traitement que des données à caractère personnel strictement nécessaires à l'exercice des missions concernées et s'effectue dans le respect de la loi relative à l'informatique, aux fichiers et aux libertés ».

834 RGPD, art. 5. c) : Les DACP doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

835 CSI, art. L. 242-4 §2.

836 CSI, art. L. 242-5 IV.

837 Pour rappel, les données à caractère personnel dites sensibles concernent « l'origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique » (LIL, art. 6 I°).

outils de reconnaissance faciale, d'autres données liées aux aspects physiques et comportementaux des individus pourraient être collectées par les drones aériens « augmentés » de sécurité publique.

331. Aussi, l'enjeu principal à l'origine des inquiétudes des défenseurs des droits et libertés repose sur le contrôle souvent inadapté de l'utilisation de ces outils et d'une collecte massive de données par les forces de l'ordre. L'adoption d'un cadre juridique régissant les usages des différents outils de vidéoprotection n'a pas suffi à répondre aux nombreux enjeux qu'ils suscitent pour les droits et libertés. En outre, l'élargissement de la législation en matière de vidéoprotection a contribué à étendre les prérogatives des forces de l'ordre, leur permettant de traiter davantage de DACP et ce de manière presque continue[838]. Face à ce constat, le président de la Commission nationale consultative des droits de l'Homme s'inquiétait du recul des droits et libertés en faveur d'une augmentation des mesures de sécurité[839] par les nombreuses dispositions législatives prises ces dernières années. En outre, il regrettait le manque de réaction face à l'accroissement des restrictions imposées aux droits et libertés. Il traduisait ce constat par le caractère « invisible » de certaines technologies ainsi que par les méthodes employées en vue de collecter des données.

332. En ce sens, les obligations relatives à l'information et à l'accès des personnes concernées par le traitement de DACP à des fins pénales peuvent faire l'objet d'exceptions dans certaines conditions sous réserve d'avoir été prévues dans l'acte instaurant le traitement et d'être une mesure nécessaire[840]. En outre, il convient de noter que l'exigence de transparence, mentionnée dans le RGPD[841], ne figure pas dans la DPJ[842]. Pour autant, la loi RPSI tend à pallier cette limitation portée aux libertés en exigeant une information générale du public s'agissant de la mise en œuvre de dispositifs de captation et d'enregistrement d'images par des caméras aéroportées[843]. Néanmoins, cette exigence n'a pas fait l'objet de précisions quant aux moyens concrets qui devront être mis en

---

838 CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 287.

839 « Les libertés fondamentales "en très mauvais état" en France, s'inquiète le président de la CNCDH », *Lamy Actualité du Droit*, 29 avril 2019.

840 DPJ, art. 13 §3 : telles qu'à des fins de maintien de la continuité d'une enquête ou procédure en cours, ou encore à des fins de protection de la sécurité publique.

841 RGPD, art. 5 §1 a).

842 DPJ, art. 4 §1 a).

843 CSI, art. L. 242-3.

œuvre[844]. De surcroît, la DPJ admet la limitation au droit d'accès, dans la mesure où elle serait « nécessaire et proportionnée dans une société démocratique »[845]. Dès lors, le manque de transparence et d'information du public ne permet pas aux personnes concernées d'avoir une connaissance éclairée de l'étendue des enjeux liés à la collecte de leurs DACP afin de faire appliquer leurs droits et de s'opposer à la massification du traitement de leurs données[846].

333. Le traitement de DACP à des fins préventives s'accorde difficilement avec les dispositions relatives à la protection des données imposant que toute collecte soit effectuée de manière non excessive[847]. Face au potentiel d'atteinte au droit à la protection des DACP que présentent les drones aériens de sécurité publique, la loi RPSI renforce cette exigence en limitant les possibilités de collecte de DACP à celles strictement nécessaires[848]. À l'instar d'autres systèmes de vidéoprotection, les drones aériens devront faire l'objet d'une analyse d'impact sur la protection des données et ne pourront être déployés qu'après la publication d'un décret ou d'un arrêté établi après avis de la CNIL[849]. Aussi, la RPSI interdit le croisement des données collectées par les drones aériens avec les fichiers de police[850]. Pour autant, elle ne s'oppose pas de manière explicite à ce que ces données puissent être inscrites dans l'un de ces fichiers suite à l'ouverture d'une procédure (autorisant le prolongement de la durée de leur conservation). Cette potentialité rejoint un enjeu plus général lié à l'augmentation exponentielle du nombre de fichiers portant sur la sécurité

---

844 Le décret n° 2023-283 du 19 avril 2023 (voir *supra*) n'apporte pas davantage de précisions sur ce point en dépit des recommandations émises par la CNIL dans son avis sur le projet de texte (CNIL, Délibération n° 2023-027 du 16 mars 2023, avis n° 22015146, *op. cit.*).

845 DPJ, art. 15.

846 CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, *op. cit.*, p. 97 ; CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *op. cit.*, p. 290 ; DELFORGE (A.) et GÉRARD (L.), « Chapitre 1. - Les robots : source de risques pour la vie privée ? » *in* DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, *op. cit.*, spéc. p. 156.

847 DPJ, art. 4 c).

848 RPSI, art. 15 et CSI, art. L. 242-4, al. 1er et 2.

849 CSI, art. L. 242-8.

850 CSI, art. L. 242-4, al. 2.

publique, ces dernières années[851].

2. Un potentiel enrichissement des fichiers de police

334. La massification de la collecte de DACP, notamment par la vidéoprotection, a grandement favorisé l'enrichissement du nombre des données pouvant être inscrites au sein des fichiers de police. De fait, la LIL comprend des dispositions spécifiques permettant la création de fichiers relatifs à la sûreté, la défense ou encore la sécurité publique[852]. Elle interdit par principe la constitution de fichiers comprenant des DACP reconnues comme sensibles au sens de son article 6 (I). Toutefois, cette interdiction fait l'objet d'une exception lorsque les traitements sont justifiés par un intérêt public moyennant l'obtention d'une autorisation préalable de l'autorité compétente (par voie législative ou réglementaire)[853]. L'intégration de DACP dans les fichiers de police n'est par conséquent pas neutre et engendre des enjeux majeurs pour les droits et les libertés[854].

335. Néanmoins, l'accroissement du nombre et du volume de ces fichiers n'a pas échappé aux yeux des défenseurs des droits et libertés et a largement participé à l'enrichissement des débats quant aux conséquences qu'ont eu le renforcement des prérogatives données aux forces de l'ordre[855]. Cette appétence des autorités publiques pour le recours au fichage massif repose principalement sur l'idée que les sociétés démocratiques sont sous la menace permanente de formes complexes d'espionnage et de terrorisme obligeant les États à surveiller de manière discrétionnaire « les éléments subversifs opérant sur son(leurs) territoire(s) »[856]. En outre, elle serait également due

---

[851] De manière non-exhaustive : BIOY (X.), Droits fondamentaux et libertés publiques, *op. cit.*, p. 551 ; LATOUR (X.) et PAUVERT (B.), Manuel de libertés publiques et droits fondamentaux, *op. cit.*, p. 235 ; LAVENUE (J-J.), « Anormalité, surveillance et fichiers de police » *in* LAVENUE (J-J.) et VILLALBA (B.), Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques, *op. cit.*, p. 237 ; BECKERICH DAVILMA (S.), « La fragilité du droit à l'oubli à l'ère des fichiers de police », in DE DAVID BEAUREGARD-BERTHIER (O.) et TALEB-KARLSSON (A.) (dir.), Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?, *op. cit.*, pp. 139-166 ; VAZ-FERNANDEZ (C-A.), Big Data et Intelligence artificielle de la sécurité intérieure en France, *op. cit.*, pp. 26-49 ; BAUER (A.) et SOULLEZ (C.), Les fichiers de police et de gendarmerie, Paris, PUF, coll. « Que sais-je ? », 2ème édition, 2011, 128 p.

[852] LIL, art. 87 à 90.

[853] LIL, art. 88 : Cette exception ouvre la possibilité à tout fichier de police de comprendre des DACP sensibles.

[854] DEFFRAINS (N.) et PLESSIX (B.), *Fichiers informatiques et sécurité publique*, Nancy, Presses Universitaires de Nancy, 2013, 241 p., p. 34.

[855] PLAZZA (P.), « L'extension des fichiers de sécurité numérique » *in* CHARDEL (P-A.), *Politiques sécuritaires et surveillance numérique*, *op. cit.*, 216 p.

[856] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 559.

à l'évolution des outils numériques en parallèle d'un accroissement de la criminalité (ou *a minima* de son constat).

336. Dans une optique de lutte contre une criminalité croissante, le législateur a mis à la disposition des autorités publiques un cadre juridique facilitant l'élaboration de fichiers informatiques, notamment la mise en œuvre de fichiers de police[857]. Les fichiers informatiques se sont ainsi progressivement imposés comme un élément indispensable à l'exercice des activités de sécurité publique. Cependant, les fichiers de police suscitent encore des interrogations quant à la diversité des types de données qu'ils peuvent contenir. Aussi, l'existence de nombreux fichiers de police constitués de DACP présente un autre enjeu tenant à la définition même de ces DACP. De fait, la définition des DACP demeure imprécise et « ne renseigne pas sur le type précis de données collectées, notamment s'il s'agit ou non de données dites sensibles. En outre, d'autres données sont collectées dans ces fichiers, comme des données relatives aux biens ou des données relatives à des éléments factuels »[858].

337. Il y a quelques années, la multiplication du nombre de fichiers de police se doublait d'un constat alarmant, celui de leur existence déloyale et parfois illégale par absence de déclaration à la CNIL. Il est arrivé que les règles juridiques tenant à la constitution de fichiers de police ne soient pas respectées et que certains fichiers aient été créés *de facto* de façon illicite[859]. En ce sens, un rapport parlementaire remis par Delphine Batho et Alain Bénisti en 2011[860] révélait que certains fichiers avaient été mis en œuvre avant d'être régularisés par une déclaration à la CNIL et d'avoir fait l'objet d'un décret en Conseil d'État ou d'un arrêté. En 2015, les publications au Journal

---

857 Ce cadre juridique repose principalement sur la Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, *op. cit.*, la LIL et la DPJ (art. 1er) mais également la jurisprudence : C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.*, cons. 20 ; CE, ass. 11 avril 2012, n° 322326, *GISTI* [en ligne] ; CE, 10ème - 9ème chambres réunies, 11 mars 2013, n° 332886, *ass. SOS Racisme* [en ligne] ; CE, 10ème - 9ème chambres réunies, 11 juillet 2016, n° 375977, *Ministre de l'Intérieur et ministre de la Défense* [en ligne]. Les traitements de données mis en œuvre pour le compte de l'État « sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté » (LIL, art. 31).

858 SYDORYK (S.), « Portrait-robot des fichiers de police », *in* DEBAETS (É.), DURANTHON (A.) et SZTULMAN (M.) (dir.), *Les fichiers de police*, Paris, LGDJ, Institut Universitaire Varenne, coll. Colloques & Essais, 2019, 425 p., p. 35.

859 *Idem*, pp. 30-31 : L'existence de certains fichiers de police pouvait être facilement dissimulée aux yeux des autorités de contrôle « ceux-ci n'ayant été ni analysés par la CNIL dans une décision, ni spécifiquement mis en place par un texte réglementaire »

860 AN, Rapport d'information n° 4113 sur « la mise en œuvre des conclusions de la mission d'information sur les fichiers de police » délivré par BATHO (D.) et BÉNESTI (J-A.) le 21 décembre 2011, 229 p., pp. 166-167 [en ligne].

Officiel de décrets portant création de nouveaux fichiers de police[861] révélaient en réalité la régularisation de fichiers de police démontrant la continuation des pratiques de créations illicites de fichiers. Aujourd'hui, les pratiques de création illégales de fichiers de police semblent avoir nettement diminuées sans pour autant avoir disparu comme en témoigne la récente mise en demeure du ministère de l'Économie concernant la création du fichier SIRENE (Système d'information du renseignement des navires et équipages) utilisé par la Direction générale des douanes[862].

338. En outre, certains fichiers de police prêtent largement à controverse allant jusqu'à remettre en question les grands principes juridiques ayant notamment trait à la politique pénale par une volonté d'accroissement des politiques de prévention des délits et des crimes. Depuis plusieurs années, l'action policière se concentre autant sur la recherche de personnes ayant commis une infraction (actions répressives) que sur les actions de prévention des actes criminels. Cependant, ces actions préventives reposent non plus sur un acte avéré mais sur la recherche de personnes potentiellement dangereuses. Face aux attaques terroristes, l'action policière tend à privilégier l'action pénale préventive (prévention répressive[863]) plutôt que la répression des infractions effectivement commises[864].

---

[861] À titre d'exemple : Décret n° 2015-1465 du 10 novembre 2015 portant création d'un traitement automatisé de données à caractère personnel relatif au suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique dénommé "CAR" mis en œuvre par la direction de l'administration pénitentiaire, *JORF* n°0263 du 13 novembre 2015 [en ligne].

[862] CNIL, Décision n° MED-2023-018 du 3 avril 2023 mettant en demeure le ministère de l'économie, des finances et de la souveraineté industrielle et numérique [en ligne] ; CNIL, « La CNIL met en demeure le ministère de l'Économie de régulariser un fichier utilisé par les douanes », *cnil.fr*, 29 mai 2023 [en ligne] ; BRANDELA (H.), « Fichier SIRENE et non-conformité à la loi Informatique et Libertés », *Village de la Justice*, 29 mai 2023 [en ligne] ; CLAVEY (M.), « La CNIL étrille le fichier illégal SIRENE de la douane maritime », *NextInpact*, 21 avril 2023 [en ligne] consultés le 21 avril 2023.

[863] PARIZOT (R.), « La distinction entre police administrative et police judiciaire est-elle déposée ? », *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, p. 140.

[864] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 562. Voir aussi : DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.* ; ALIX (J.), « La lutte contre le terrorisme entre prévention pénale et prévention administrative », *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, pp. 154-155. Sur l'orientation « préventive » prise par l'action policière, voir notamment : Décret n° 2020-1512 du 2 décembre 2020 concernant le traitement de données à caractère personnel dénommé *Gestion de l'information et prévention des atteintes à la sécurité publique* (GIPASP), *JORF* n°0293 du 4 décembre 2020 [en ligne] ; Décret n° 2020-1510 du 2 décembre 2020 à propos du traitement de données à caractère personnel *Enquêtes administratives liées à la sécurité publique* (EASP), *JORF* n°0293 du 4 décembre 2020 [en ligne] ; Décret n° 2020-1511 du 2 décembre 2020 sur le traitement de données à caractère personnel titré *Prévention des atteintes à la sécurité publique* (PASP), *JORF* n°0293 du 4 décembre 2020 [en ligne] : Ce fichier vise ainsi à collecter des informations sur « des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique » et « a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles de prendre part à des activités terroristes, de porter atteinte à l'intégrité du territoire ou des institutions de la République ou d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives » (art. 1er).

339. La finalité de ce type de fichiers de police vient ainsi modifier la conception de la procédure pénale où « l'on passe de la recherche de comportements anormaux, […] à la recherche de ce que l'on considérera comme une anormalité de comportement dans le cadre d'une surveillance préventive globale portant sur la totalité de la population »[865]. Le comportement « anomal » ne sera alors plus associé à un « standard social » (sens commun de l'anormalité) mais reposera sur la conception qu'en aura le concepteur de l'algorithme équipant une caméra ou les autorités publiques. L'inquiétude que suscite ces fichiers de police est accentuée du fait qu'ils ne ciblent plus uniquement des personnes ayant commis des actes illégaux mais toute personne considérée comme potentiellement dangereuse au motif de vouloir assurer la protection des personnes et des biens. Certains fichiers sont ainsi directement liés à la délinquance tandis que d'autres ne portent pas directement à la commission d'une infraction, tels les fichiers relatifs aux renseignements généraux. Cette multiplication des fichiers de police laisse planer un risque significatif de surveillance globale des personnes[866]. En outre, les finalités distinctes, aussi précises et encadrées soient-elles, des fichiers de police, n'entravent nullement la possibilité d'une augmentation du nombre de fichiers et du fichage des personnes.

340. Dès lors, les fichiers de police intéressent autant les missions de police préventive que répressive et ne se limitent pas au recensement de DACP de personnes poursuivies puisque des « éléments de toutes natures et concernant l'ensemble des personnes mentionnées dans une procédure (personne mise en cause, témoins, victimes) peuvent y figurer, dès lors qu'ils sont utiles à la compréhension d'un dossier »[867]. Aussi, même lorsque les données ne sont pas identifiantes[868], le fait de les collecter de manière massive présente toujours la potentialité de permettre *a minima*

---

[865] LAVENUE (J-J.), « Anormalité, surveillance et fichiers de police », p. 236 *in* LAVENUE (J-J.) et VILLALBA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, *op. cit.*

[866] *Idem*, pp. 243-244. Voir aussi : CEDH, gd ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n°58170/13, 62322/14 et 24960/15 [en ligne] et CE, ass., 21 avril 2021, n° 393099, 394922, 397844, 397851, 424717, 424718, *French data Network et a.* [en ligne].

[867] *Idem*, p. 24-25.

[868] Pour rappel, les données sont qualifiées de non personnelles lorsqu'elles ne comprennent pas d'informations reconnues par les textes ou la jurisprudence comme étant à caractère personnel (Règlement (UE) 2018/1807 du parlement européen et du conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *op. cit.*, art. 3 : Les données à caractère non personnel sont définies comme « toutes les données autres que les données à caractère personnel au sens de l'article 4, point 1), du RGPD »). Il en va ainsi des données anonymisées. Le procédé d'anonymisation peut être défini comme « le résultat du traitement de données personnelles afin d'empêcher, de façon irréversible, toute identification » (G29, Avis 05/2014 sur les Techniques d'anonymisation, *op. cit.*, p. 3). Ainsi, les données anonymisées sont considérées comme non identifiantes.

l'individualisation d'une personne[869]. L'application du droit de la protection de la vie privée et des DACP doit ainsi être analysée au regard des finalités du traitement des données (y compris non personnelles).

341. Le constat d'une multiplication et d'une variété des types de données collectées laisse ainsi craindre une forme de surveillance généralisée où chaque individu serait potentiellement le suspect d'une infraction. Dès lors, les drones aériens « augmentés » de sécurité publique participent indubitablement à l'aggravation des limitations portées aux droits et libertés à commencer par le droit à la protection de la vie privée et aux DACP. En outre, cette technologie sera confrontée aux cybermenaces qui pourront porter préjudice tant à l'outil lui-même qu'aux données qu'il collecte.

§2. Les potentialités d'atteintes à l'intégrité des drones aériens de sécurité publique

342. Le développement et la multiplication des systèmes d'information (SI) se conjuguent avec l'accroissement du nombre et de l'incidence des cybermenaces[870] permettant d'exploiter des failles de sécurité, en d'autres termes les vulnérabilités d'un SI. L'existence de vulnérabilités

[869] Le suivi effectué par un drone aérien de sécurité publique d'un individu suspecté d'avoir commis une infraction pourrait entrer dans le cadre de la définition d'une individualisation en offrant la possibilité d'isoler une partie ou la totalité des données au milieu de la masse afin d'extraire des facteurs pertinents permettant d'identifier un individu. En ce sens, l'avis 05/2014 sur les techniques d'anonymisation du G29 révélait qu'il était encore complexe pour les experts du domaine de garantir avec certitude que les données ont effectivement fait l'objet d'une anonymisation irréversible par les processus d'anonymisation existants. Voir aussi sur ce sujet : VIANGELLI (F.), « Des données à la responsabilité : de l'anonymisation à l'attaque par réidentification », *RLDI* n° 173, août-septembre 2020, pp. 40-45.

[870] Le règlement européen en matière de cybersécurité, dit « Cybersecurity Act », qualifie de cybermenace « toute circonstance, tout évènement out toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes » (Règlement (UE) 2019/881 du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), *JOUE* du 7 juin 2019, art. 2, 8) [en ligne]).

informatiques et les conséquences des cyberattaques[871] ne sont aujourd'hui plus à démontrer[872]. En ce sens, Jean-Claude Junker déclarait, lors de son discours devant le Parlement européen sur l'état de l'Union du 13 septembre 2017, que « les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars » ajoutant qu'elles « ne connaissent pas de frontières [et] n'épargnent personne »[873]. La vulnérabilité des SI revêt de multiples enjeux de souveraineté, d'ordre économique ou encore juridique qui entrent dans le cadre étendu de la cybersécurité[874]. En ce sens, les nombreuses vulnérabilités auxquelles peuvent être sujets les SI sont susceptibles de porter atteinte à leurs données qui peuvent faire l'objet d'une diffusion, d'une modification ou encore d'une suppression. Or, ces atteintes portées aux données ont une incidence significative sur les droits et libertés lorsqu'elles portent sur des personnes. Dès lors, le recours aux SI dans le cadre de la sécurité publique, si évident soit-il, nécessite de prendre des précautions contre les nombreuses et diverses cyberattaques[875].

---

[871] L'auteur Amos Guiora définit une cyberattaque comme « un acte d'agression délibéré et direct visant à porter atteinte à des infrastructures critiques. En outre, il s'agit de toute tentative délibérée de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des ressources, ou des procédés par l'utilisation de moyens électroniques » (N. GUIORA (A.), *Cybersecurity : Geopolitics, law, and policy,* New-York, Routledge, 2017, p. 17). L'auteur Olivier Kempf identifie plusieurs éléments permettant de qualifier une cyberattaque considérant qu'elle peut cibler trois « niveaux » d'une technologie : la couche matérielle du cyberespace (ex. infrastructures de réseau, ordinateurs, etc.), la couche logique (ex. systèmes d'exploitation, logiciels, protocole du réseau, etc.) et la couche sémantique (à savoir principalement les données) (KEMPF (O.), *Introduction à la cyberstratégie*, Paris, Economica, 2ème édition, 2015, 236 p., p. 10-16).

[872] L'existence même du Code de la cybersécurité en est un éminent témoignage, de même que l'organisation du Forum Internationale pour la Cybersécurité (FIC) qui se déroule chaque année à Lille. De manière non-exhaustive plusieurs ouvrages et articles effectuent une analyse des enjeux relatifs à la cybersécurité et des moyens permettant de se prémunir des cyberattaques notamment : ARPAGIAN, (N.), *La cybersécurité*, Paris, PUF, coll. Que sais-je, 2022, 128 p. ; AVOINE (G.) et KILLIJIAN (M-O.) (dir.), *13 défis de la cybersécurité*, Paris, CNRS Editions, 2020, 262 p. ; FÉRAL-SCHUHL (C.), *Cyberdroit : Le droit à l'épreuve de l'internet*, Paris, Dalloz, 8e édition, 2020, 1888 p. ; GORRIEZ (F.), *Le droit de la cybersécurité*, Paris, Éditions Nuvis, 2019, 225 p. ; DE MAISON ROUGE (O.), *Les cyberisques : La gestion juridique des risques à l'ère de l'immatérielle*, Paris, LexisNexis, 2018, 192 p. ; QUÉMÉNER (M.), *Cybercriminalité : droit pénal appliqué*, Paris, Economica, 2010, 273 p. ; Dossier « Comment réagir en cas de cyberattaque ? », *Dalloz IP/IT* n°7-8, 24 juillet 2021 ; CAPRIOLI (É.), « Vers un marché unique des acteurs de la cybersécurité », *Communication Commerce électronique* n° 5, mai 2019 ; PINTE (J-P.), Blog « Cyberisques, cybercriminalité et nouveau monde » [en ligne].

[873] Président Jean-Claude Juncker, « Discours sur l'état de l'Union 2017 », Bruxelles, 13 septembre 2017 [en ligne].

[874] Au sens de l'Agence nationale de sécurité des systèmes d'information (ANSSI), la cybersécurité peut être entendue comme « l'état recherché pour un système d'information qui lui permet de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données qui sont stockées et traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles » (ANSSI, « Glossaire » [en ligne] consulté le 14 octobre 2022). En d'autres termes, la cybersécurité repose sur des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et la cyberdéfense. Elle doit répondre à trois objectifs généraux : la disponibilité, l'intégrité et la confidentialité (UIT, « Présentation générale de la cybersécurité », 18 avril 2008, p. 3 [en ligne]). Le *Cybersecurity Act* définit la cybersécurité comme toutes « actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces » (Règlement (UE) 2019/881 du 17 avril 2019, *op. cit.*, art. 2 1)).

[875] PELLEGRINI (F.), « Sécurité et numérique - Entre fantasmes d'efficacité et violations avérées des droits fondamentaux », pp. 89-100, p. 89 *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*

343. La généralisation des attaques informatiques - Les cybermenaces portent atteinte autant au secteur privé qu'au secteur public, sans oublier les particuliers. Les attaques portées aux institutions ou aux structures étatiques[876] ont des conséquences particulièrement néfastes, celles-ci étant susceptibles de mettre en péril le fonctionnement de SI essentiels à la vie de la nation. Ces attaques peuvent notamment avoir pour objectif de provoquer le dysfonctionnement de structures reconnues comme étant des opérateurs d'importance vitale[877] ou encore d'instances gouvernementales. La première cyberattaque ayant ciblé une structure étatique s'est déroulée le 27 avril 2007 en Estonie[878]. Cette attaque par déni de service (*DDoS*[879]), à l'aide de *botnets*[880] usant de réseaux d'ordinateurs zombies, visait les serveurs web estoniens provoquant « des effets dévastateurs sur les systèmes d'information dus à l'arrêt des services en ligne »[881]. Cette attaque aura permis de faire prendre conscience aux différents gouvernements de l'ampleur des enjeux liés à la cybersécurité et s'est notamment matérialisée par la rédaction du premier Manuel de Tallin par un groupe d'experts mandatés par l'Organisation Transatlantique Nord (OTAN)[882].

---

876 Voir pour exemple : Sénat, Rapport d'information n° 82 sur la sécurité informatique des pouvoirs publics délivré par BASCHER (J.) le 22 octobre 2019 [en ligne].

877 Les opérateurs d'importance vitale sont définis comme « les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative » (Code de la défense, art. L. 1332-1). L'ANSSI les désigne comme ceux qui « exerce[nt] des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ; gère[nt] ou utilise[nt] au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population » [en ligne].

878 « La Russie impliquée dans la cyber-attaque contre l'Estonie ? », *journaldunet.com*, 1er juin 2007 [en ligne] ; CROUZILLACQ (P.), « L'Estonie dénonce les cyber-attaques terroristes russes », *01net.com*, 11 juin 2007 [en ligne] ; IFRAH (L.), « Analyse de la première attaque massive des systèmes d'information d'un Etat », *Revue Défense Nationale* n°700, septembre 2007, pp. 104-114 [en ligne] consultés le 28 novembre 2022.

879 Déni de service distribué (*Distributed Denial of Service*) : « action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu » (ANSSI, « Glossaire » [en ligne] consulté le 5 décembre 2022). Lorsque ce déni de service provient d'une attaque celle-ci peut provenir d'un bombardement de courriels (*mailbombing*) ou d'un *botnet*.

880 « Un *botnet* (ou réseaux de machines zombies) est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise » (ANSSI, Glossaire, [en ligne]).

881 IFRAH (L.), « Analyse de la première attaque massive des systèmes d'information d'un Etat », *op. cit.* : La panique s'est étendue au-delà des frontières estoniennes atteignant les plus hautes échelles des États de la communauté internationale.

882 Le premier Manuel de Tallin fut publié par l'OCDE en 2013. Dans un souci d'adéquation avec l'évolution des enjeux relatifs à la cybersécurité un deuxième Manuel vit le jour en 2017. Actuellement, le Centre d'excellence de la coopération pour la cyberdéfense de l'OCDE travaille sur une troisième version du Manuel de Tallin. Centre d'excellence de la coopération pour la cyberdéfense, « Manuel de Tallin » [en ligne].

344. Plusieurs autres attaques informatiques ont également pris pour cible des institutions ou des structures étatiques telles les attaques par sabotage *Stuxnet* en 2009-2010[883] et *NotPetya* en 2017[884]. De même, plusieurs institutions gouvernementales américaines, à l'instar de l'Agence de sécurité des États-Unis (*Department of Homeland Security*) ou encore le Département de la Justice des États-Unis ont été victimes de la cyberattaque *SolarWinds*[885]. En 2022, le FBI avait publié une notification indiquant que différentes agences gouvernementales locales avaient été victimes d'attaques par rançongiciels perturbant de nombreux services essentiels durant l'année 2021 et au début de l'année 2022[886]. Selon une étude publiée en avril 2021[887], les institutions gouvernementales et les organismes de régulation constitueraient 12% des victimes des cyberattaques[888]. Les États font fréquemment face à des attaques visant leurs systèmes d'information[889]. Le caractère essentiel et permanent des SI des services publics n'a également pas échappé aux cybers attaquants et suscite pleinement leur attention[890]. Ce constat démontre le besoin vital d'élever le maintien d'une sécurité informatique constante et de haut niveau au rang des

---

883 Pour plus d'information sur cette cyberattaque : N. GUIORA (A.), *Cybersecurity : Geopolitics, law, and policy, op. cit.*, p. 35 and pp. 48-51 ; ZETTER (K.), *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New-York, Crown Publishing Group, 2014.

884 L'attaque NotPetya aurait pu être assimilée à un rançongiciel mais était en réalité destinée à effacer les données. Cette cyberattaque mondiale s'est répandue dans des milliers d'entreprises. Le logiciel malveillant empêchait les données d'être décryptées notamment par l'intermédiaire d'une fausse demande de rançon. Pour plus d'informations voir notamment : GREENBERG (A.), "The Untold story of notpetya, the most devastating cyberattack in history", August 22nd 2018 [en ligne] ; BRUMFIELD (C.), « 5 ans après, quelles leçons tirer des attaques NotPetya », *Lemondeinformatique*, 4 juillet 2022 [en ligne] consultés le 1er décembre 2022

885 Les attaquants sont parvenus à pénétrer les SI de ces agences leur permettant, par la suite, d'avoir notamment accès aux adresses mails par l'intermédiaire d'un code malveillant dissimulé dans les mises à jour de logiciels utilisés. Celui-ci a permis d'infecter les produits de l'entreprise *SolarWinds* (un des principaux fournisseurs de solutions logicielles des institutions gouvernementales américaines) et ainsi de donner aux attaquants un accès au réseau des organisations ayant recours à ces logiciels afin de soustraire des informations (SUDERMAN (A.), "SolarWinds hack got emails of top DHS officials", *AP News*, 29 March 2021 [en ligne] ; CIMINO (V.), « Piratage SolarWinds : les hackers ont eu accès aux e-mails du DHS (Department of Homeland Security) », *Siècle Digital,* 30 mars 2021 [en ligne] consultés le 30 mars 2021).

886 Cybersecurity & Infrastructure Security Agency (CISA), "FBI Releases PIN on Ransomware Straining Local Governments and Public Services", March 31st 2022 [en ligne] ; PALMER (D.), « Aux Etats-Unis, les ransomwares s'attaquent aux services publics », *ZDNet*, 1er avril 2022 [en ligne] consultés le 2 avril 2022.

887 Mc GUIRE (M.), "Nation States, Cyberconflict and the Web of Profit", University of Surrey, April 2021 [en ligne].

888 *Idem*, p. 15.

889 Le système d'information et de communication de l'État est défini à l'article 1er du décret n° 2019-1088 du 25 octobre 2019, *JORF* n°0251 du 27 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique [en ligne] comme étant « composé de l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique les données qui concourent aux missions des services de l'État et des organismes placés sous sa tutelle » Annexe 6 de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics, *JORF* n°0253 du 30 octobre 2022 [en ligne].

890 PALMER (D.), « Aux Etats-Unis, les ransomwares s'attaquent aux services publics », *op. cit.*

priorités absolues.

345. Dernièrement, les chercheurs en cybersécurité s'inquiètent de l'émergence d'attaques sur les microprogrammes[891]. Différentes tentatives de piratage à visée spécifique ont été recensées, à l'image de celles ayant pour objectif d'entraver les activités d'agences gouvernementales[892]. Les entités publiques, y compris les plus hautes institutions, ne sont pas à l'abri de ces attaques et peuvent même constituer une forme de *challenge* pour les attaquants. Les différentes attaques informatiques ayant eu lieu depuis le début de cette décennie rappellent qu'aucune entité privée comme publique ne sera épargnée dans cette guerre dématérialisée. Les différents acteurs liés de près ou de loin à l'univers numérique en ont d'ailleurs pris conscience et nombre d'entre eux répètent qu'il ne s'agit pas de savoir si une entité va être victime ou non d'une attaque informatique mais plutôt de savoir quand et comment se préparer au mieux pour y faire face[893]. Tous les outils numériques et, par conséquent, toutes les données informatisées sont susceptibles de faire l'objet d'une attaque informatique.

346. La cybervulnérabilité des caméras de surveillance - Les systèmes de vidéoprotection peuvent également présenter différentes formes de vulnérabilités. Outre les difficultés de continuité d'activité, ces attaques présentent un double enjeu juridique en portant atteinte tant à l'intégrité de l'outil connecté qu'aux données collectées[894]. Les conséquences d'une telle vulnérabilité pourraient être considérables en ce qu'elles rendraient irrecevables les données collectées dans le cadre d'une procédure judiciaire. En outre, elles sont susceptibles de remettre en question toute la chaine de la

---

[891] À l'image de *Lojax*, un programme informatique capable de se situer au niveau le plus profond de l'appareil connecté par l'intermédiaire de l'interface UEFI (*Unified Extensible Firmware Interface*) qui permet l'amorçage et le chargement du système d'exploitation. De part son emplacement, le logiciel malveillant ne peut être supprimé par un processus de réinstallation ou même par effacement du disque dur et compromet alors de manière durable le système d'exploitation. Bien que rares, ces types d'attaques ne doivent pas être négligées et constituent une nouvelle forme de « cyber-arme ».

[892] Pour exemple, l'attaque de la chaîne d'approvisionnement américaine *Sunburst* en 2020 aura permis aux protagonistes de pénétrer dans les systèmes d'information des agences gouvernementales clés telles que le ministère américain de la Sécurité intérieure, le département d'État américain, les instituts nationaux américains de la santé, le ministère américain du Commerce et le ministère américain du Trésor (Mc GUIRE (M.), "Nation States, Cyberconflict and the Web of Profit", *op. cit.,* p. 15).

[893] GORRIEZ (F.), *Le droit de la cybersécurité*, *op. cit.*, p. 9.

[894] *Idem*, p. 151 : L'ANSSI classifie les vulnérabilités des systèmes de vidéoprotection en trois catégories : l'atteinte à la confidentialité des données, l'atteinte à la disponibilité du système de vidéoprotection et l'intrusion dans le reste du système d'information. Cette dernière catégorie, assez générale, renferme notamment les atteintes au troisième pilier de la cybersécurité concernant l'intégrité des données.

preuve pénale allant de la loyauté de la collecte des données[895] à leur recevabilité au procès pénal compte tenu du manquement au principe de garantie d'intégrité des données issues de ces caméras.

347. Les drones aériens de sécurité publique présentent des vulnérabilités similaires dans la mesure où ils collectent massivement des données, dont des DACP. Or, la réglementation en matière de protection des DACP impose à tout responsable de traitement le respect du principe de précaution qui implique d'assurer la sécurité et la confidentialité des données[896]. Les drones aériens de sécurité publique doivent donc être soumis à des mesures de sécurité accrues permettant de protéger les données collectées. L'emploi de drones aériens de sécurité publique nécessite *de facto* une prise de conscience des agents quant aux diverses possibilités de prise de contrôle du drone par un tiers (qui pourrait potentiellement permettre de modifier son programme ou ses fonctionnalités) et d'atteintes aux données collectées. Aussi, dans le cadre de la sécurité des drones aériens de sécurité publique, il importe autant d'assurer l'intégrité de l'objet en lui-même (A) que les SI et centres d'hébergement qui traitent et stockent les données (disponibilité des SI et intégrité des données traitées) (B).

A. Le détournement des drones aériens de sécurité publique

348. Nonobstant les qualités technologiques dont ils disposent, les drones aériens demeurent vulnérables à de nombreux types d'attaques. Cette vulnérabilité peut prendre plusieurs formes. Les attaques peuvent porter atteinte à l'outil en lui-même, telles que celles visant à endommager, détruire ou neutraliser le drone. Elles peuvent également cibler les systèmes du drone, telles que la fréquence radio ou la liaison satellite, permettant le contrôle du drone et le transfert des données collectées, ou encore la caméra assurant la collecte des images. Les drones aériens sont des objets connectés par nature[897]. Or, les experts en cybersécurité admettent qu'il s'avère encore

---

[895] Les opérateurs perdraient de fait le contrôle de l'utilisation de l'outil de vidéoprotection et *de facto* de la collecte des données.

[896] RGPD, art. 32 ; DPJ, art. 29 ; LIL, art. 4 6°, 34 et 99. En ce sens, la LIL dispose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (art. 34).

[897] De fait, les drones aériens reçoivent leurs instructions de navigation aérienne du télépilote par voie d'émission et les données qu'ils collectent font également l'objet d'une transmission. Voir notamment : PIETTE-COUDOL (T.), *Les objets connectés : Sécurité juridique et technique*, Paris, Édition LexisNexis, 2015, 126 p., p. 55 ; Episode #376 « Sécurité des drones », *nolimitsecu.fr*, 17 juillet 2022 [Podcast en ligne] ; « Cybersécurité des drones : entretien avec Victor Vuillard, CSO et CTO cybersecurité de Parrot », *InCyber*, 22 novembre 2022 [en ligne].

particulièrement complexe de parer les attaques portées aux objets connectés[898]. Dans le cas des drones aériens l'inconvénient pourrait provenir de leur mauvaise sécurisation.

349. Ces différents facteurs sont à l'origine de multiples vulnérabilités qui n'auront pas manqué d'être exploitées, notamment lors d'une attaque ayant permis de paralyser un réseau complet de vidéoprotection. En 2014, l'attaque du botnet *Miraï* (en d'autres termes un réseau zombie[899]) aura ainsi marqué le domaine de la vidéoprotection en affectant un réseau entier de caméras de surveillance disposées partout dans le monde et destiné à filmer la voie et les lieux publics[900]. Cette attaque par déni de service (*DDoS*) avait permis d'entraver le fonctionnement du système par saturation[901]. Révélée par la société Imperva[902], cette attaque avait démontré l'importance de mettre en œuvre des dispositifs techniques et organisationnels de sécurité quel que soit le type d'outil connecté. Ces révélations ont souligné un cruel manquement aux normes de sécurité des détenteurs de ces caméras. Aussi, les drones aériens peuvent présenter des vulnérabilités similaires ainsi que de nouvelles résultant de leur caractère mobile (1). En ce sens, différents cas d'attaques ont déjà été recensés (2).

1. Les cybervulnérabilités des drones aériens de sécurité publique

350. Le détournement des drones aériens est une potentialité inhérente tant à leur caractère mobile qu'à leur connectivité. Les télépilotes usent de moyens de télécommunication (généralement des ondes radio) leur permettant d'assurer une connexion entre un émetteur au sol et le drone aérien afin de transmettre des commandes et des instructions de navigation. Afin d'assurer la liaison et la transmission des données entre eux et le centre de contrôle, les drones aériens militaires et d'État

---

898 BISEUL (X.), « Comment se prémunir contre les attaques d'objets connectés « zombies » », *Journal du net*, 23 novembre 2016 [en ligne].

899 Les réseaux zombies se composent de machines interconnectées (en réseau) qui agissent sous le contrôle d'un ou de plusieurs attaquants.

900 MARION (J-Y.), « Les virus informatiques », pp. 107-108 *in* AVOINE (G.) et KILLIJIAN (M-O.) (dir.), *13 défis de la cybersécurité*, *op. cit.*

901 AVOINE (G.) et KILLIJIAN (M-O.) (dir.), *13 défis de la cybersécurité*, *op. cit.*, p. 107.

902 Impervia, « CCTV DDoS Botnet In Our Own Back Yard », 21 October 2015 [en ligne] ; « Détournement des caméras de vidéo-surveillance en botnet », *Undernews*, 4 novembre 2015 [en ligne].

usent de canaux satellitaires, d'ondes radios ou télécom[903].

351. La transmission et le stockage des données collectées par les drones de sécurité publique peuvent s'effectuer selon deux procédés. Soit les données sont transmises directement vers le centre de commandement (sans stockage préalable) soit elles sont stockées dans la mémoire du drone aérien afin d'être examinées ultérieurement. Ces deux options présentent, l'une comme l'autre, des atouts mais aussi des risques pour les données. Dans le premier cas, les données stockées dans la mémoire du drone aérien encourent de possibles atteintes à leur intégrité, disponibilité et confidentialité en cas d'attaque portée directement sur celui-ci (ex. prise de contrôle ou capture par une personne ou un groupe malveillant). Dans le deuxième cas, les données sont transmises directement au centre de commandement et peuvent être sujettes à une attaque portée sur le mode de transmission des données (ex. interception du flux de données, brouillage du signal, etc.).

2. Les différentes typologies d'attaques pouvant affecter les drones aériens de sécurité publique

352. Les attaques portant sur des drones aériens reposent sur deux types de finalités. D'une part, elles peuvent affecter la navigabilité ou le contrôle d'un drone aérien. D'autre part, elles sont susceptibles de porter atteinte aux flux de données transitant entre l'aéronef et le poste de commandent aux fins d'empêcher leur transmission, de les modifier, de les détruire ou encore à des fins d'espionnage par interception des données. De nombreux exemples permettent d'illustrer les attaques auxquelles les drones aériens de sécurité publique pourraient faire face.

353. Parmi les différents types d'attaque, l'une consiste à perturber la fréquence des ondes radioélectriques afin de prendre le contrôle de l'appareil, de le rediriger et d'avoir accès aux données collectées[904]. De fait, les ondes radioélectriques permettent la liaison entre un télépilote et un drone aérien et peuvent être interceptées ou perturbées de diverses manières, notamment par des interférences dues à une usurpation de la liaison ou par brouillage[905]. Un autre type d'attaque vise à

---

[903] EDDAZI (F.), « La cybervulnérabilité des drones militaires : enjeux du combat numérique », p. 200 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

[904] DOARÉ (R.), DANET (D.) et DE BOISBOISSEL (G.), *Drones et killer robots : Faut-il les interdire ?*, *op. cit.*, p. 178.

[905] Le brouillage de signaux satellitaires (*spoofing* en anglais) consiste à altérer les communications et le réglage d'un émetteur sur une fréquence identique afin d'annuler le signal initial pour le substituer par celui de l'attaquant. Cette technique peut s'avérer particulièrement efficace en vue d'intercepter un drone aérien.

brouiller les signaux des systèmes de navigabilité entrainant la perte de contrôle du drone ou de ses données. Certains drones aériens comprennent un dispositif GPS dont les informations permettent de déterminer leur localisation et d'assurer leur navigabilité[906]. Toutefois, un signal GPS peut être vulnérable aux interceptions et être aisément endommagé, bloqué ou détourné par des tiers malveillants[907]. En 2012, Todd E. Humphreys avait eu recours à ce procédé dans le cadre de ses recherches et était parvenu à détourner un drone en utilisant un dispositif de mystification (ou *spoofer*) permettant d'envoyer de faux signaux GPS au système de pilotage[908]. En 2018, un spectacle lumineux de drones aériens à Hong Kong avait été victime d'un dispositif de brouillage de leur signal GPS causant la chute des appareils[909]. Certains drones aériens militaires ont été équipés de dispositifs permettant de les prémunir de ce type d'attaque[910]. Aussi les drones aériens déployés en essaims seraient plus résistants aux attaques portées aux signaux GPS[911].

354. Enfin, il serait encore possible de prendre le contrôle d'un drone à l'aide d'un logiciel informatique ou d'une simple application de smartphone. Des tests en ce sens avaient été effectué lors des Drone-Games de 2012 où des développeurs de l'entreprise Groupon avaient modifié les instructions d'un drone « afin qu'il prenne en photo le public, utilise un outil de reconnaissance faciale puis tweete la photo avec le nom de la personne lorsque celle-ci était identifiée »[912]. Dès lors, l'interception des fréquences radio ou de tout autre mode de transmission des images, vidéos et autres données collectées par les drones ne constitue pas qu'une éventualité et doit être prise en compte dans le processus de gestion des risques. En 2016, la presse informatique avait rapporté qu'un chercheur, Jonathan Anderssen, était parvenu à pirater et à prendre le contrôle de drones en

---

906 Le signal GPS permet au télépilote de localiser le drone aérien et de le maintenir sous son contrôle y compris hors de son champ de vision.

907 GUINIER (D.), « Sécurité : Vulnérabilité aux cyberattaques du GPS à usage civil », *Expertises des systèmes d'information* n°3, mars 2017, pp.108-112. Voir aussi : SMYTH (S.), *Drone controversies : ethical and legal debates surrounding targeted strikes and electronic surveillance*, Toronto, Thomson Reuters, 2016, 146 p., p. 101 : Il est possible de brouiller le signal GPS d'un drone aérien et de causer la perte du signal par son télépilote laissant la possibilité à l'attaquant d'en prendre le contrôle à ses fins.

908 GUINIER (D.), « Sécurité : Vulnérabilité aux cyberattaques du GPS à usage civil », *op. cit.*

909 Mc CARTHY (S.), ZHENG (W.) and TSANG (D.), "HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show", *South China Morning Post*, 29 October 2018 [en ligne] ; NICHOLS (G.), "Cheap GPS jammers a major threat to drones", *zdnet.com*, 14 December 2020 [en ligne] consultés le 5 décembre 2022.

910 HAMBLING (D.), *Swarm Troopers : How small drones will conquer the world*, Archangel Ink Press, 2016, 322 p., p. 266.

911 SMYTH (S.), *Drone controversies : ethical and legal debates surrounding targeted strikes and electronic surveillance*, *op. cit.*, p. 101.

912 CNIL, « Drones, innovations, vie privée et libertés individuelles », *op. cit.*

exploitant une faille de sécurité de leur protocole DSMx utilisé pour le pilotage à distance à l'aide d'un boîtier de contrôle prénommé Icarus[913].

355. Certaines attaques ont pour principal objectif d'usurper le contrôle du drone aérien. En 2011, un drone américain avait fait l'objet d'une capture par les autorités iraniennes qui étaient parvenues à couper la liaison entre le drone et sa base de contrôle et à interrompre la liaison satellite du GPS afin de transmettre d'autres coordonnées GPS au drone, le redirigeant vers l'Iran[914]. En 2014, la presse avait relaté une attaque informatique sur les serveurs logistiques de drones ayant temporairement perturbé la liaison entre la France et ses aéronefs lors du survol de l'Afghanistan en 2011[915].

356. D'autres attaques visaient plus spécifiquement les données transitant entre le drone et le centre de commandement. Ainsi, en 2009, des images issues des caméras de drones américains avaient été captées par des insurgés irakiens par l'intermédiaire d'un logiciel ayant intercepté, faute de chiffrement[916], les flux vidéo entre les drones et leur base opérationnelle[917] leur permettant de suivre les appareils et de déterminer quelles zones du pays faisaient l'objet d'une surveillance par l'armée américaine[918]. En 2011, une autre attaque avait cette fois visé la station de contrôle au sol de drones américains dans le Nevada par l'intermédiaire d'un virus informatique ayant permis d'usurper le contrôle du cockpit par l'intermédiaire d'un programme malveillant d'espionnage

---

913 BARTHE (O.), « Icarus, le boîtier capable de pirater les drones », *lemondeinformatique.fr*, 28 octobre 2016 [en ligne] ; ZAFFAGNI (M.), « Icarus, le boîtier qui peut pirater n'importe quel drone en plein vol », *futura-sciences.com*, 3 novembre 2016 [en ligne].

914 EDDAZI (F.), « La cybervulnérabilité des drones militaires : enjeux du combat numérique », p. 199 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.* ; EASTON (R.) and FRAZIER (E.), "GPS Declassified : From Smart Bombs to Smartphones", *Technology and Culture* 57 (1), January 2016, pp. 276-278 [en ligne] ; MICK (J.), "Iran: Yes We Hacked the U.S's Drone and Here's How we Did It", *Daily Tech*, 15 December 2011 [en ligne] consulté le 5 décembre 2022.

915 GUILLERMARD (V.), « L'armée investit pour lutter contre les cybermenaces », *Le Figaro*, 6 juin 2014 [en ligne] consulté le 5 décembre 2022.

916 GORMAN (S.), DREAZEN (Y. J.), COLE (A.), "Insurgents hack US Drones", *Wall Street Journal*, 17 December 2009 [en ligne] consulté le 5 décembre 2022.

917 EDDAZI (F.), « La cybervulnérabilité des drones militaires : enjeux du combat numérique », p. 199 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

918 Mc CULLAGH (D.), "U.S Was Warned of Predator drone Hacking", *CBS News*, 17 December 2009 [en ligne] consulté le 5 décembre 2022.

(*keylogger*) alors que les drones survolaient l'Afghanistan et d'autres zones de conflit[919]. Enfin, en 2016, un autre article de presse révélait que la *National Security Agency* (NSA) et le *Government Communications Headquarters* (GCHQ) étaient parvenus à intercepter les liaisons entre des drones israéliens et leurs satellites par l'intermédiaire d'une attaque portée au logiciel de chiffrement des images[920]. Ces exemples ont, toutefois, permis aux développeurs d'anticiper ces possibilités d'atteinte et d'intégrer dès la conception des techniques de sécurité permettant de protéger tant les appareils (drones et stations de contrôle) que les données collectées (ex. chiffrement de bout en bout des flux de données).

357. La cybervulnérabilité des drones aériens de sécurité publique doit être au cœur des préoccupations de leurs utilisateurs compte tenu de la gravité qu'engendrerait sur les droits et libertés une atteinte portée à l'intégrité du drone ou de ses données. Cette cybervulnérabilité avait déjà fait l'objet de mesures dans le domaine des drones aériens militaires lors de la rédaction du *Livre blanc sur la défense et la sécurité nationale* de 2013[921]. Le texte classait en ce sens la cybervulnérabilité comme étant le troisième risque majeur à prendre en considération dans le cadre de la mise en œuvre de la stratégie de défense et de sécurité nationale. D'autres institutions ont également pris la mesure des potentielles cybervulnérabilités des drones aériens et des conséquences qu'elles engendreraient sur les données collectées (personnelles ou non personnelles). En ce sens, le G29[922] avait émis un avis en juin 2015 concernant la protection des DACP dans le cadre d'une utilisation de drones aériens[923]. Il avait souligné la gravité que présenterait une usurpation par des tiers malveillants d'outils connectés, plus spécifiquement dans le cas où ceux-ci

---

[919] SMYTH (S.), *Drone controversies : ethical and legal debates surrounding targeted strikes and electronic surveillance*, *op. cit.*, p. 102 : Les experts du service de sécurité des réseaux militaires n'avaient pas été en mesure d'affirmer avec certitude que ce virus avait été introduit de manière intentionnelle ou par accident ni même de connaitre l'étendue de son champ d'action. En revanche, ils avaient confirmé que le virus avait indifféremment affecté des données confidentielles comme non confidentielles et aurait potentiellement porté atteinte à la confidentialité des données par l'intermédiaire du programme d'espionnage qui aurait par la suite diffusé les données sur Internet à des personnes hors de la chaine de commandement militaire. Voir aussi : SHACHTMAN (N.), "Computer Virus Hit U.S. Drone Fleet", *Wired*, 17 July 2011 [en ligne] consulté le 5 décembre 2022.

[920] CURRIER (C.), MOLTKE (H.), "Spies in the sky. Israeli drone feeds hacked by British and American Intelligence", *The Intercept*, 29 January 2016 [en ligne] consulté le 5 décembre 2022.

[921] Ministère de la Défense, Rapport « Livre blanc sur la défense et la sécurité nationale 2013 » remis par GUÉHENNO (J-M.), 29 avril 2013, 160 p. [en ligne].

[922] Le G29 était le groupe européen chargé d'émettre des avis et recommandations en matière de protection des DACP remplacé par le Comité européen de protection des données (CEPD/*EDPB*) depuis l'entrée en vigueur du RGPD.

[923] G29, Avis n° 01/2015 sur la vie privée et les problématiques de données personnelles au regard de l'utilisation des drones du 16 juillet 2015, 21 p. [en ligne].

appartiendraient à l'État.

B. La cybervulnérabilité des données issues des drones aériens de sécurité publique

358. Les données collectées par les drones aériens de sécurité publique peuvent également être sujettes aux cybermenaces. Aussi, la vigilance en matière de sécurité informatique des drones aériens de sécurité publique concerne aussi la protection des SI qui stockent les données qu'ils collectent. De fait, celles-ci font l'objet d'un traitement par les SI du centre de commandement où elles sont transférées. En outre, elles peuvent être conservées sur le long terme dans des centres d'hébergement de données. L'ampleur prise par la multiplication des attaques informatiques et l'appétence de certains attaquants pour les données sensibles au sens du RGPD[924] révèle l'importance primordiale de renforcer les mesures en matière de sécurité informatique. S'agissant des drones aériens de sécurité publique, la sécurisation des données s'effectue à plusieurs niveaux allant de la collecte à leur transmission au centre de commandement puis tout au long de leur conservation éventuelle notamment dans des centres d'hébergement de données. Ces données peuvent être conservées dans des serveurs au sein du centre de commandement ou dans des serveurs externes[925] (ou *cloud*) compte tenu de la quantité de données. Le recours à des serveurs externes peut présenter des opportunités de sécurité des données[926] autant que des contraintes[927]. Les atteintes portées aux données issues des drones aériens de sécurité publique sont susceptibles d'advenir tout au long du cycle du traitement et peuvent engendrer de graves conséquences pour les droits des personnes concernées (1). Des cas récents démontrent que les services institutionnels font également l'objet de cyberattaques visant leurs données (2).

---

924 À titre d'exemple : les données relatives au domaine de la défense dans le cadre d'une opération d'espionnage, les données relatives à la santé à des fins d'usurpation ou d'escroquerie par un rançongiciel, ou encore les données relatives aux condamnations pénales et aux infractions.

925 BENSAMOUN (A.), *Les Robots : Objets scientifiques, objets de droits*, Lyon, éditions Mare & Martin, 2016, 236 p., p. 156.

926 Selon les recommandations de l'ANSSI, la règle de trois qui permet d'assurer l'accessibilité des données suppose de conserver celles-ci sur trois supports différents situés dans des endroits différents (ex. cloud, disque dur externe, dossier papier, etc.) [en ligne].

927 Le *cloud computing* présente de grandes capacités de stockage et facilite le partage d'informations (tel que dans le cadre de la coopération policière). Toutefois, il peut parfois encore susciter certaines réserves quant aux dispositifs de sécurité et, plus particulièrement, quant à la localisation des serveurs. Ainsi, le manque de transparence et l'importante dépendance aux entreprises technologiques (majoritairement étrangères à l'Union européenne) témoignent d'un certain manque de contrôle sur les données qui *in fine* impacte la confiance des différents acteurs impliqués (v. **n° 765 et suiv.**).

1. Les potentialités d'atteintes aux données des drones aériens de sécurité publique

359. Les cyberattaques à l'encontre des données constituent une violation de la sécurité du système de traitement des données. Elles peuvent notamment avoir pour objectif un détournement des finalités du traitement. Les failles de sécurité peuvent conduire à une violation des DACP définie par la LIL comme « toute violation de la sécurité entrainant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel »[928]. Cette définition se limite aux données identifiantes mais la violation de données peut également porter sur des données non personnelles. De fait, les capteurs dont seront équipés les drones aériens de sécurité publique ont pour objectif de collecter une importante quantité de données, qu'il s'agisse de DACP ou de données non personnelles. Aussi, toute faille de sécurité subie par un drone aérien de sécurité publique engendrerait de graves conséquences à la sauvegarde de l'ordre public dans le cadre des missions des forces de l'ordre mais aussi à l'exercice des droits et libertés des personnes.

360. En matière de drones aériens, il n'existe pas de règles spécifiques permettant de réprimer la violation des données ou la prise de contrôle par un tiers malveillant à l'exception du principe général de prudence issu de la réglementation en matière de drones à usage civil[929]. Toutefois, le droit commun dispose d'un arsenal de règles en matière de lutte contre la cybercriminalité. Les dispositions relatives à la répression des atteintes aux systèmes de traitement automatisé de données (STAD)[930] peuvent s'appliquer en matière de lutte contre les atteintes portées aux données faisant l'objet d'un traitement par les drones aériens de sécurité publique. Ces dispositions, issues de la loi relative à la fraude informatique dite « Godfrain » du 5 février 1988[931], sont codifiées dans le Code

---

928 LIL, art. 83.

929 Voir en ce sens : CHARLES (J-B.) et PARIER (S.), « Les drones dans le viseur des cybercriminels : que dit le droit ? », *Air & Cosmos* n° 2555, 7 juillet 2017, p. 25 [en ligne].

930 Les systèmes de traitement automatisés de données (STAD) ne font l'objet d'aucune définition législative. Seuls les débats parlementaires permettent d'en donner une définition comme étant « tout ensemble composé d'une ou de plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs déterminés » (Sénat, Texte n°27, 1987-1988, 4 novembre 1987, p. 2 [en ligne]). Un STAD peut également être défini comme « l'ensemble des éléments physiques et des programmes utilisés pour le traitement des données, ainsi que ceux qui permettent d'établir la communication entre les différents éléments d'un système et […] tous les vecteurs de transmission de données » (BENSOUSSAN-BRULÉ (V.) et TORRES (C.), *Failles de sécurité et violation des données personnelles*, Bruxelles, éditions Larcier, coll. Manuels Larcier, 2016, 134 p., p. 123).

931 Loi n° 88-19 du 5 janvier 1988 relative aux infractions des systèmes de traitement automatisé de données, *JORF* du 6 janvier 1988.

pénal et définissent cinq types d'infractions pouvant être portées aux STAD[932]. Deux de ces infractions s'avèrent particulièrement pertinentes pour qualifier les attaques portées aux drones aériens de sécurité publique, qu'il s'agisse de l'outil lui-même ou de ses données.

361. En premier lieu, la prise de contrôle d'un drone aérien pourrait entrer dans le cadre de l'infraction portant sur l'atteinte à l'intégrité d'un STAD. Cette infraction dispose de fait d'un spectre large permettant d'intégrer tout type de pratiques frauduleuses : attaque DDoS par déni de service[933], implantation et usage de *botnets*, les logiciels malveillants ou encore les virus, pour ne citer qu'eux. En deuxième lieu, la violation des données issues des drones aériens peut être qualifiée d'atteinte aux données d'un STAD qui repose sur le fait « d'introduire frauduleusement des données » ou, à l'inverse, « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement » les données d'un STAD[934]. Il faut noter que cette disposition réprime tout acte frauduleux sur les données d'un STAD qu'il donne lieu à un dommage ou non. Dans un arrêt du 8 décembre 1999, la Cour de cassation est venue préciser la notion de délit d'atteinte à l'intégrité des données, énonçant que toute modification ou suppression frauduleuse des données contenues dans un STAD était constitutif d'un délit « sans qu'il soit nécessaire que les modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système ni que leur auteur soit animé de la volonté de nuire »[935]. Elle estime par conséquent que la démonstration du caractère intentionnel n'est pas nécessaire à la qualification de l'infraction. L'atteinte portée aux données d'un STAD constitue un acte grave car il vise l'intégrité de ces données. Dans le cas des drones aériens de sécurité publique, les attaques ciblant les données auront pour conséquence d'entacher la recevabilité de la preuve. De fait, pour être recevable dans le cadre d'une procédure judiciaire, les données traitées par les drones aériens de sécurité publique devront être collectées de manière loyale et ne pas avoir été altérées que ce soit de manière accidentelle ou frauduleuse (atteinte à l'intégrité des données)[936].

---

[932] Code pénal (CP), art. 323-1 et suiv. : l'accès ou le maintien frauduleux dans un STAD, l'atteinte à l'intégrité d'un STAD, l'atteinte à l'intégrité des données d'un STAD, la détention, l'offre, la cession ou la mise à disposition d'un équipement d'atteinte aux STAD, et l'association de malfaiteurs.

[933] TGI de Paris, 19 mai 2006 et TGI de Bordeaux, 6 janvier 2011.

[934] CP, art. 323-3. Cette disposition a, par ailleurs, fait l'objet d'une modification afin d'étendre le champ des comportements pouvant être constitutifs de cette infraction (Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, *JORF* n°0263 du 14 novembre 2014, art. 16 [en ligne]).

[935] C. cass., ch. crim., 8 décembre 1999, n° 98-84.752 [en ligne].

[936] CSI, art. L. 242-2, al. 2 (garantie d'intégrité des enregistrements) et art. L. 242-3 (information du public).

2. Les typologies d'atteintes aux données des services institutionnels

362. En dépit du haut niveau de sécurité informatique dont bénéficient les services institutionnels, ceux-ci ne sont donc pas invulnérables aux cyberattaques, qu'il s'agisse d'attaques par sabotage[937] ou par espionnage[938]. Ces dernières années, plusieurs exemples relatés par la presse permettent de démontrer les cybervulnérabilités dont peuvent être victimes les SI des forces de l'ordre. Le 8 juin 2021, un article du journal *Volkskrant*[939] révélait ainsi que la police néerlandaise a fait l'objet d'un piratage de ses systèmes informatiques par un service de renseignement russe. Cette attaque fut identifiée, non pas par la police victime de l'attaque mais, par le service de renseignement extérieur des Pays-Bas. Cette attaque aurait été perpétrée par le service de renseignement militaire russe qui aurait entrepris de s'infiltrer au sein des SI de la police néerlandaise suite à une enquête qu'elle aurait lancée concernant l'explosion du vol MH17 en Ukraine impliquant la Russie. Suite aux recommandations des services de renseignement néerlandais, la police néerlandaise serait parvenue *in fine* à « bouter hors du système »[940] et à effacer toute trace des espions moyennant, néanmoins, un investissement conséquent.

363. En France, plusieurs institutions ont également fait l'objet d'attaques diverses. En 2022, le ministère de la Justice aurait été victime d'un piratage de ses données[941]. En 2023, plusieurs organismes français ont subi des attaques par DDoS revendiquées par un groupe de pirates informatiques pro gouvernement russe[942]. En mars, ce sont l'Assemblée nationale et le Sénat qui ont subit le même type d'attaque[943]. Les attaques seraient menées contre les sites officiels des États membres de l'UE en représailles au soutien qu'ils accordent à l'État Ukrainien. Aussi, la question de la vulnérabilité des données policières peut être illustrée de manière très concrète par l'attaque

---

937 Le sabotage peut avoir pour effet de modifier ou de supprimer les données (atteinte à l'intégrité des données), d'empêcher ou de ralentir l'accès aux données (atteinte à l'accessibilité des données).

938 L'espionnage constitue une atteinte à la confidentialité des données pouvant être sanctionné comme étant constitutif d'une infraction par accès ou maintien frauduleux dans un STAD au sens de l'article 323-1 du CP.

939 MODDERKOLK (H.), « Russen zaten ten tijde van mh17 onderzoek door hack diep in systemen politie », *Volkskrant*, 8 juin 2021 [en ligne].

940 « Le renseignement russe avait piraté la police néerlandaise », *NextInpact*, 18 juin 2021 [en ligne].

941 VITARD (A.), « Le Ministère de la Justice victime d'un ransomware ? », *Usine Digitale*, 28 janvier 2022 [en ligne].

942 BODNAR (B.), « Des hackers russes s'attaquent à la France pendant le discours de Poutine », *Numerama*, 21 février 2023 [en ligne] consulté le 27 mars 2023.

943 BODNAR (B.), « Le site de l'Assemblée nationale en panne après une cyberattaque de hackers russes », *Numerama*, 27 mars 2023 [en ligne] ; BIGET (S.), « Le site de l'Assemblée nationale mis K.-O. par des hackers russes », *Futura Sciences*, 27 mars 2023 [en ligne] consultés le 27 mars 2023.

informatique de la police et de l'armée Suisse en juin 2023[944]. L'attaque perpétuée à l'encontre du fournisseur d'accès internet de ces deux institutions aurait ainsi permis la récupération de fichiers confidentiels[945].

364. Ces révélations illustrent, parmi d'autres, la preuve de la vulnérabilité des SI des institutions étatiques, dont celles des forces de l'ordre. Ces attaques n'entendent pas nécessairement porter atteinte à l'accessibilité du SI ou même à l'intégrité des données. En revanche, elles impliquent presque systématiquement une atteinte au troisième pilier tenant à la sécurité informatique que constitue la confidentialité des données. Ces cybermenaces ont par conséquent un triple effet, celui de rendre potentiellement inutilisable les SI, ou de rendre les données inexploitables mais aussi de remettre en question l'application concrète des mesures permettant d'assurer la confidentialité des données. Cette dernière vient dès lors entièrement remettre en cause l'obligation tenant aux forces de l'ordre de limiter de manière stricte l'accès aux données qu'elles collectent aux seules personnes habilitées. De fait, l'accès par des personnes non-autorisées à des données confidentielles (telles que celles collectées dans le cadre d'une enquête judiciaire ou encore celles inscrites dans les fichiers de police) porte indubitablement atteinte au droit à la protection de la vie privée des personnes et au respect de leurs données à caractère personnel. Au-delà d'une violation de l'obligation de confidentialité, les informations pouvant être soustraites par les attaquants pourraient ultérieurement faire l'objet d'une utilisation à des fins malveillantes et porter un préjudice conséquent aux personnes concernées.

365. En vertu des règles relatives à la protection des DACP, le responsable de traitement doit assurer le respect des finalités du traitement en assurant notamment la sécurité des DACP[946]. En ce sens, une décision de la CEDH du 20 juin 2023, se référant à la décision du 22 juin 2021 de la CJUE[947], affirmait que « le traitement de données à caractère personnel relatives à des infractions pénales appelle une protection renforcée en raison de la sensibilité particulière des données en cause

---

944 MARIN (J.), « La police et l'armée suisses victimes collatérales d'une cyberattaque », *Usine Digitale*, 5 juin 2023 [en ligne] ; SEYDTAGHIA (A.), « Une cyberattaque hors norme frappe la Suisse, touchant l'armée et de nombreuses polices », *Le Temps*, 2 juin 2023 [en ligne] consultés le 5 juin 2023.

945 *Idem* : « Une attaque visant un prestataire informatique a permis à des hackers de dérober des documents de la police fédérale et de l'armée suisse. Des milliers de fichiers confidentiels ont déjà été publiés sur Internet ».

946 RGPD, art. 5 §1 f) et 32 ; DPJ, art. 4 §1 f) et 29.

947 CJUE, gr. ch., 22 juin 2021, *Latvijas Republikas Saelma*, C-439/19 [en ligne].

»[948]. Dès lors, les forces de l'ordre et les services de secours effectuant une collecte de DACP dans le cadre de l'utilisation d'un drone aérien devront préalablement identifier les risques que ce traitement peut engendrer et mettre en œuvre des mesures de sécurité adéquates. En d'autres termes, les failles de sécurité devront être anticipées par une équipe composée de spécialistes en protection des données et en gestion des risques liée à la violation de ces données tels que le responsable des systèmes d'information (RSSI) et le délégué à la protection des données (DPD ou *DPO*[949]).

366. Aussi, les effets sur les droits et les libertés sont susceptibles d'être amplifiés par l'association des drones aériens de sécurité publique aux algorithmes « augmentés » d'aide à la décision. Une grande part des enjeux entourant l'utilisation de systèmes algorithmiques dans le domaine policier a déjà été identifiée. D'une manière générale, l'enjeu principal repose sur une insuffisance de contrôle de ces usages tant sur le plan technique que juridique qui incite à la méfiance du grand public.

Section 2 De nouvelles limitations des droits et libertés induites par les drones aériens « augmentés » de sécurité publique

367. Ces dernières années, les progrès technologiques ont ouvert une branche très en vogue dans le domaine des algorithmes, celle de l'apprentissage machine (*machine learning*). Ces nouvelles capacités permettent à une machine d'apprendre à partir de données issues de situations réelles. Ces algorithmes peuvent ainsi être utilisés dans des contextes très variés, allant de la classification de données à la prévision d'évènements afin d'aider les utilisateurs dans leurs prises de décision.

368. Le recours aux systèmes d'aide à la prise de décision (SAAD) associés aux dispositifs de vidéoprotection relève désormais de l'évidence pour les autorités publiques tant cette technologie est susceptible de faciliter les tâches des agents des forces de l'ordre dans leurs missions de prévention des infractions et de recherche de leurs auteurs. Pourtant, ces technologies ne sont pas exemptes de défauts pouvant conduire à des atteintes aux droits et libertés des individus filmés et

[948] CEDH, 20 juin 2023, *Margari c/ Grèce*, n° 36705/16, § 59 [en ligne]. Voir comm. SUDRE (F.), « Droit au respect de la vie privée - Protection des données personnelles dans le cadre d'une procédure pénale », *JCP-G* n° 26, 3 juillet 2023, act. 810.

[949] Il est plus courant d'employer l'acronyme anglo-saxon *DPO* signifiant *Data Protection Officier*.

analysés. Les exemples qui ont pu être observés à l'étranger témoignent des dérives que peuvent engendrer l'utilisation incontrôlée et opaque de ces technologies par les forces de l'ordre à des fins préventives comme répressives[950].

369. À titre d'exemple, le recours à l'algorithme d'IA COMPAS[951] par les forces de l'ordre aux États-Unis afin d'estimer les potentialités de récidives avait fait grand bruit suite à la publication d'un article scientifique en 2016[952] démontrant le caractère raciste, et donc discriminant, des résultats que produisait son algorithme. L'algorithme n'était capable de produire des résultats corrects que dans 61% des cas. Les auteurs de l'article avaient ainsi dénoncé le fait que l'algorithme produisait des résultats nettement plus négatifs envers les Noirs qu'envers les Blancs. D'après leurs analyses, l'algorithme produisait plus souvent de faux-positifs à l'encontre des Noirs, estimant qu'ils allaient récidiver plutôt que non récidiver, qu'à l'encontre des Blancs. En outre, les résultats produits s'agissant des Blancs avaient une forte tendance à produire deux fois plus de faux-négatifs estimant qu'ils allaient moins récidiver[953]. L'algorithme produisait ainsi des résultats discriminants à l'encontre des Noirs en sur-évaluant les possibilités qu'ils récidivent et en sous-évaluant les possibilités de récidives des Blancs[954].

370. Depuis quelques années, l'usage des technologies d'IA suscite des réserves de la part de certains scientifiques à l'instar du célèbre astrophysicien Stephen Hawking qui affirmait que

---

950 De manière non-exhaustive : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, spéc. 99-108 ; OSWALD (M.), GRACE (J.), URWIN (S.) AND BARNES (G.), "Algorithmic risk assessment policing models : lessons from the Durham HART model an 'experimental' proportionality information & communications technology law", *Information & Communications Technology Law*, August 31st 2017 ; GRGIĆ-HLAČA (N.), REDMILES (E. M.) GUMMADI (K. P.) and WELLER (A.), "Human Perceptions of Fairness in Algorithmic Decision Making: A Case Study of Criminal Risk Prediction", *in WWW 2018: The 2018 Web Conference*, April 23–27 2018, 10 p. [en ligne] ; RICHARDSON (R.), "Community Forum on Algorithmic Bias", *AI Now Institute*, December 7th, 2019 [en ligne] ; "Biometric Surveillance Is Quietly Expanding: Bright-Line Rules Are Key", *AI Now Institute*, April 11th 2023 [en ligne] ; ARTE THEMA, « Prédire les crimes », *op. cit.* ; McCABE (D.), "NOVA : Prediction by the Numbers", *op. cit.*
Voir en ce sens les actions menées par l'*American Civil Liberties Union* (ACLU) concernant les technologies de surveillance à l'usage des forces de l'ordre aux États-Unis [en ligne] notamment l'article de STANLEY (J.), "The Dawn of Robot Surveillance : AI, Video, Analytics, and Privacy", *op. cit.* et "Community Control Over Police Surveillance : Technology 101", *ACLU*, September 16th 2016 [en ligne].
Certaines actions ont ainsi été entreprises à l'encontre de l'usage de ces technologies par des organisations de protection et de défense des droits et libertés aux États-Unis telles que la *Community Control Over Police Surveillance* [en ligne].

951 COMPAS : Correctional Offender Management Profiling for Alternative Sanctions.

952 LARSON (J.), ANGWIN (J.), MATTU (S.) and KIRCHNER (L.), "Machine Bias", *ProPublica*, May 23rd 2016 [En ligne].

953 HOANG (LN.) et EL MHAMDI (EM.), *Le fabuleux chantier : Rendre l'intelligence artificielle robustement bénéfique*, *op. cit.*, p. 42.

954 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », Fondation Abeona et Paris Télécom, février 2019 [en ligne].

« l'intelligence artificielle pourrait mettre fin à l'humanité »[955]. Les développements de l'IA suscitent des inquiétudes notamment quant aux conséquences que cette technologie peut avoir sur la vie privée et soulèvent de nombreuses questions d'ordre éthique[956]. De même, certains acteurs issus du secteur des technologies de l'information et de la communication s'inquiètent des conséquences que pourrait avoir l'usage de l'IA en l'absence de toute réglementation adéquate[957]. Néanmoins, il convient de garder une certaine lucidité dans l'analyse des enjeux que suscitent les technologies d'IA en fonction de leurs usages afin de ne pas porter de jugement disproportionné et erroné ou à l'inverse de l'idéaliser[958]. En ce sens, le ministre délégué chargé de la Transition du numérique français, Jean-Noël Barrot, déclarait s'agissant de l'algorithme d'IA ChatGPT qu'il ne fallait ni le plébisciter comme une solution miracle ni l'interdire par crainte[959]. Les craintes suscitées par le recours aux technologies d'IA peuvent s'expliquer de différentes manières[960]. Parmi ces explications la « loi d'Amara » traduit une « tendance à surestimer l'incidence d'une nouvelle technologie à court terme et à la sous-estimer à long terme »[961]. Aussi, il serait erroné et contreproductif de vouloir surestimer les capacités d'une technologie et de sous-estimer celles des êtres humains. En ce sens, le professeur Philippe Besse, questionné sur le sujet des discriminations algorithmiques, affirme que « des décisions algorithmiques ne sont pas plus objectives que des

---

955 HAWKING (S.), « L'intelligence artificielle pourrait mettre fin à l'humanité », *Le Monde et AFP*, 3 décembre 2014 [en ligne] consulté le 23 février 2023.

956 BESSE (P.), CASTETS-RENARD (C.) et GARIVIER (A.), « Loyauté des décisions algorithmiques », Contribution au débat public initié par la CNIL : Éthique et Numérique, 22 juin 2017 [en ligne].

957 Voir notamment : RUIZ (P.), « Le développement de l'IA sans réglementation induit une menace existentielle pour l'humanité », *developpez.com*, 17 février 2023 [en ligne] consulté le 23 février 2023.

958 Le Conseil d'État affirmait ainsi que « parce qu'elle véhicule aussi un imaginaire angoissant voire apocalyptique […] l'intelligence artificielle s'expose, plus encore que bien d'autres instruments de l'action publique, à des contestations et des remises en cause potentiellement irrationnelles voire violentes, et donne prise à des thèse complotantes sur le thème de la surveillance et de la manipulation généralisées » (CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 94). De même, des chercheurs et développeurs en informatique estiment ainsi que « sans nier que l'automatisation puisse avoir un impact nécessitant un niveau de réflexion propre, il semble nécessaire de veiller à ne pas sombrer dans un technocentrisme qui masquerait l'héritage intellectuel de la critique de la bureaucratie, attribuant ainsi aux algorithmes tous les problèmes dus à la complexité, à l'opacité ou à l'absurdité des décisions prises » (PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *INRIA*, 14 mai 2018, p. 7 [en ligne]).

959 « La technologie n'est ni bonne ni mauvaise en soi, elle est toujours au service de l'Homme [et] comme tout outil technologique, elle présente un certain nombre de risques qu'il faut pouvoir maîtriser » (ROLLAND (S.) et MABILLE (P.), Interview de Jean-Noël Barrot, ministre de la Transition numérique « Non, il ne faut pas interdire ChatGPT », *La Tribune*, 6 avril 2023 [en ligne] consulté le 11 avril 2023).

960 BROOKS (R.), « Pourquoi l'intelligence artificielle nous fait autant fantasmer », *Courrier international*, 20 décembre 2017 [en ligne] ; « L'IA : révolution ou véritable danger ? (partie 1/2) », *Boursorama*, 14 avril 2021 [en ligne] consultés en septembre 2021.

961 Adage de Roy Amara, cofondateur de l'*Institute for the Future* (IFTF) de Palo Alto au cœur de la Silicon Valley.

décisions humaines[962]. […] les biais humains sont fidèlement reproduits voire amplifiés même si la variable sensible (genre, origine, âge, etc.) est absente de la base de données »[963].

371. Aussi, les avancées dans le domaine de l'IA nécessitent de saisir pleinement toutes les implications de cette technologie et de ses applications, ce qui peut s'avérer parfois extrêmement complexe. Il est essentiel d'avoir conscience des effets tant intentionnels que non intentionnels des technologies d'IA. Bien que le recours à l'IA repose généralement sur des intentions louables, il faudra garder à l'esprit que les effets de cette technologie peuvent ne pas toujours correspondre aux attentes de leurs concepteurs comme de leurs utilisateurs. Il arrive que certaines technologies développées avec de bonnes intentions présentent des effets négatifs tels que le renforcement de discriminations à l'égard de certaines personnes ou de groupe de personnes dû aux résultats biaisés d'un algorithme. La prise en compte de ces aspects lors de la conception de ces technologies et lors de l'évaluation de leurs impacts et de leurs applications est donc primordiale[964].

372. Il convient désormais d'identifier les différents enjeux entourant la conception et l'utilisation d'algorithmes « augmentés » à des fins de sécurité publique. Certains d'entre eux sont communs à tous les algorithmes quand d'autres sont spécifiquement liés à leur utilisation à des fins préventives et répressives. Dans sa résolution du 6 octobre 2021, le Parlement européen identifiait trois catégories de risques que pouvait engendrer l'usage de l'IA par les forces de l'ordre[965]. Les deux premiers risques soulignés par le Parlement européen sont les biais algorithmiques et le défaut de robustesse de cette technologie qui peuvent entrer dans le cadre plus général tenant à l'insuffisante fiabilité qu'il est possible d'accorder à cette technologie (§1). Le troisième risque concerne les enjeux de cybersécurité spécifique à l'IA (§3).

373. À ceux-ci peuvent s'ajouter des enjeux relatifs à l'opacité de l'usage de ces technologies par les forces de sécurité publique, incluant notamment l'effet « boîte noire » (§2). Il s'agit d'une

---

962 Pour exemple : DE-ARTEAGA (M.) *et al.*, "Bias in Bios: A Case Study of Semantic Representation Bias in a High-Stakes Setting", *ACM Conference on Fairness, Accountability, and Transparency*, January 27th 2019 [en ligne] ; BESSE (P.) *et al.*, "A Survey of Bias in Machine Learning Through the Prism of Statistical Parity", *The American Statistician*, July 2nd 2021, pp. 188-198 [en ligne].

963 VALLET (F.), « Philippe Besse : Les décisions algorithmiques ne sont pas plus objectives que les décisions humaines, *linc.cnil.fr*, 2 juin 2020 [en ligne].

964 HAYDA (M.) and RAKOVA (B.), "Enhanced well-being assessment as basis for the practical implementation of ethical and rights-based normative principles for AI", *op. cit.*

965 Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*, points 8, 9 et 11 et cons. M.

absence de connaissance et de compréhension du fonctionnement et des conséquences de l'usage de ces technologies principalement due au nombre restreint de spécialistes de ces algorithmes au sein de la population générale[966]. Ces enjeux soulèvent la question de la légitimité de l'utilisation de ces technologies, principalement dans un cadre préventif. Les enjeux soulevés par les algorithmes « augmentés » à l'usage de la sécurité publique sont donc nombreux, tant du point de vue technique que juridique et éthique. Bien qu'il soit impossible de concevoir des algorithmes parfaits il est nécessaire d'identifier pour chaque type et usage d'algorithme les verrous subsistants et d'apporter une solution au cas par cas afin de réduire au mieux les atteintes qu'ils peuvent engendrer sur les individus.

§1. La fiabilité limitée des algorithmes « augmentés »

374. Le développement d'un algorithme basé sur l'apprentissage automatique[967] nécessite une base d'apprentissage[968]. Celle-ci se compose d'une observation d'entrée et d'une observation de sortie[969]. L'observation d'entrée repose sur un ensemble de données quantifiables dont l'algorithme se servira pour effectuer ses calculs. L'observation de sortie correspond au résultat que devrait fournir l'algorithme en fonction des données qu'il aura eu à analyser. Originairement, cette observation dépend de l'expertise d'une personne issue du domaine dans lequel évoluera l'algorithme. Le modèle[970] d'apprentissage automatique permet ainsi d'apprendre et de reproduire

---

966 ISOARD (G.), « Algorithmes et biais cognitifs », p. 92 *in* DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.*

967 L'apprentissage automatique (*machine learning*) constitue un « ensemble d'algorithmes, sous ensemble de l'IA, mimant les capacités humaines d'apprentissage et d'entrainement » (CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 67). Il s'agit d'un sous-domaine de l'IA dans lequel les algorithmes apprennent à partir de données.

968 L'apprentissage est « un sous-domaine de l'IA qui consiste à produire automatiquement un modèle à partir d'un grand ensemble de données dites d'apprentissage » (DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 260). Il existe plusieurs formes d'apprentissages tels que l'apprentissage supervisé (annotation des données d'apprentissage avec le résultat attendu ; technique assez fastidieuse), l'apprentissage non supervisé (constitution de modèles à partir des données) ou encore l'apprentissage continu (en employant un apprentissage par renforcement où une « récompense » est délivrée à la machine en fonction de l'adéquation de sa réponse au résultat attendu).

969 PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *Dalloz IP/IT* n°2, 19 février 2022, p. 75.

970 Le modèle peut être défini comme « la logique utilisée par le système pour réaliser des prédictions ou préconiser des décisions » et « peut être plus ou moins compréhensible pour un humain » (DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 263).

cette expertise[971]. L'apprentissage automatique d'un algorithme repose sur un modèle mathématique qui comprend plusieurs paramètres. Ces paramètres peuvent être ajustés afin de modifier les prédictions de sortie en fonction des données en entrée.

375. Aussi nombreux soient les avantages que présentent les algorithmes d'apprentissage automatique, ce modèle d'apprentissage comporte aussi des écueils, principalement dans le cadre de décisions ayant une incidence sur des êtres humains. L'usage d'algorithmes « augmentés », particulièrement dans le domaine pénal, requière une grande fiabilité technologique[972]. Ces algorithmes nécessitent de nombreuses données pour produire des résultats. Dès lors, ces résultats dépendent de la qualité des données sur lesquelles reposent leurs calculs, qu'il s'agisse des données d'apprentissage comme des données d'entrée durant son utilisation. La « qualité » des données repose sur plusieurs facteurs : leur qualité technique (ex. qualité des images issues des systèmes de vidéoprotection), leur intégrité, leur adéquation au contexte d'utilisation, etc.

376. Ainsi, la fiabilité des algorithmes d'aide à la prise de décisions est un enjeu crucial. De fait, l'existence de biais est susceptible d'engendrer à terme un résultat erroné pouvant porter préjudice aux personnes concernées. De même, les données collectées durant la mission peuvent s'avérer insuffisantes ou sujettes à interprétation et conduire l'algorithme à produire un résultat peu fiable. Aussi, les données d'apprentissage constituent des éléments importants qui, lorsqu'elles sont erronées ou insuffisantes, entrainent de faux résultats de l'algorithme. Dès lors, le manque de fiabilité que peuvent encore présenter les algorithmes « augmentés » utilisés à des fins de sécurité publique, laisse craindre de potentielles atteintes aux droits et libertés et plus particulièrement au droit à la sûreté[973]. Ce manque de fiabilité peut résulter d'erreurs de l'algorithme (A) ou encore de biais algorithmiques (B).

---

971 PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

972 Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 59 et suiv. Voir aussi : Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*, §§ 8 et 9 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 108-112 ; LELIEUR (J.), « L'intelligence artificielle : une nouvelle technologie probatoire en émergence », *AJP* n° 3, 30 mars 2023, p. 112.

973 En ce sens le Sénat affirmait que « l'usage d'algorithmes peu performants rend, dans le meilleur des cas, [les technologies d'analyse d'images] inopérante[s] et risque, dans le pire des cas, de décupler les atteintes aux droits et libertés publiques » (Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 59).

A. Les erreurs algorithmiques des technologies de surveillance de sécurité publique

377. Les algorithmes d'IA présentent encore des erreurs et souffrent d'un manque de robustesse qui peuvent à l'usage contrevenir à leur efficacité ainsi que porter atteinte aux droits et libertés. Il convient de rappeler que les algorithmes sont conçus par des êtres humains ; or, l'être humain est un être faillible et par conséquent les résultats rendus par un algorithme peuvent présenter des erreurs[974].

378. La mesure de fiabilité des algorithmes s'effectue sur des critères de taux (vrai positif, faux positif, vrai négatif, faux négatif) qui permettent d'estimer leur pourcentage d'erreurs. Les algorithmes peuvent être sujets à deux catégories d'erreurs réciproquement liées : les taux de faux positifs et ceux de faux négatifs. Les taux de faux positifs correspondent aux alertes émises par l'algorithme qui ne répondent pas aux attentes de l'utilisateur ou qui ne sont pas conformes. À l'inverse, les taux de faux négatifs correspondent à l'absence d'alerte de l'algorithme. En d'autres termes, les concepteurs doivent estimer si les taux de vrais positifs ou de vrais négatifs[975] sont suffisants pour déclarer l'outil comme présentant une fiabilité suffisante. Il appartient au concepteur d'effectuer la configuration de l'algorithme au préalable en fonction du seuil de tolérance de l'un des deux taux et de la pertinence quant aux finalités d'utilisation. Dès lors, si un algorithme d'analyse d'images de caméras de vidéoprotection est conçu afin de détecter la présence interdite d'individus dans un espace défini il sera programmé de manière à avoir une tolérance faible aux faux positifs.

379. Les erreurs issues des algorithmes peuvent avoir plusieurs origines. La fiabilité de l'algorithme repose sur la qualité de sa conception et de ses conditions d'entraînement qui dépendent notamment du nombre et de la diversité des jeux de données d'entraînement. Les résultats d'un algorithme peuvent être erronés en raison des données sur lesquelles reposent ces calculs. De fait, la qualité des données utilisées lors de la phase d'apprentissage du logiciel est

---

974 MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.* : « Les modèles d'apprentissage peuvent potentiellement reproduire et aggraver les discriminations » (p. 98). De fait, le recours aux algorithmes « augmentés » « loin de neutraliser les biais qui existent déjà […] contribuent sans nul doute à les renforcer par leur effet inévitablement performatif » (p. 108) ; BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, . 9 : « Les résultats des algorithmes dépendent de la manière dont les programmeurs les ont écrits. Or, ces derniers restent des êtres humains » tous sujets à des biais cognitifs dans leur prise de décision.

975 En d'autres termes, lorsque ce qui apparait dans le résultat correspond aux attentes (vrai positif) ou lorsque ce qui est exclu du résultat correspond aux attentes (vrai négatif).

déterminante. Dans le cas de l'analyse d'images issues de caméras, leur cadrage, leur résolution ou encore les conditions météorologiques ont une incidence sur la qualité des données de l'image. Les erreurs peuvent aussi provenir du codage de l'algorithme[976] ; en d'autres termes, de la conception de l'algorithme en lui-même sans tenir compte de ses données d'apprentissage. Enfin, les biais sont une source d'erreurs de l'algorithme en produisant des performances plus ou moins différentes selon certains critères (âge, sexe ou encore origine ethnique du sujet).

380. La fiabilité d'un algorithme est par conséquent conditionnée par celle de ses données ; en d'autres termes par l'assurance de leur intégrité, de leur nombre, de leur diversité, de leur qualité et de leur exactitude (véracité). De fait, les algorithmes nécessitent un entrainement préalable sur des jeux de données dites « d'apprentissage » afin d'obtenir des résultats suffisamment fiables[977]. Cela suppose l'exclusion des données erronées qui risqueraient de compromettre la chaîne de calculs de l'algorithme ainsi que celles de ses prochaines opérations (par réaction en chaîne). La fiabilité des données est par conséquent un enjeu aussi crucial que complexe s'agissant de déceler une donnée erronée (particulièrement lorsque celles-ci sont analysées en masse).

381. Une autre difficulté s'agissant de la fiabilité des algorithmes réside au sein même des laboratoires de recherche, plus particulièrement s'agissant des publications scientifiques. Afin d'évaluer l'efficacité de leurs algorithmes les chercheurs s'appuient sur la théorie de la valeur-p développée par Ronald Fisher en 1920. Cette théorie consiste à utiliser une valeur-p[978], autrement dit une probabilité, comme indicateur pratique de succès. Les chercheurs et concepteurs d'algorithmes se vouent une concurrence acharnée les contraignant à ne vouloir publier que leurs succès car ces publications sont essentielles pour leur carrière. Aussi, « la tentation de maquiller et manipuler les données expérimentales en une bonne valeur-p est considérable. Il existe un terme pour cela : le p-hacking »[979]. Le « p-hacking » consiste donc à altérer les résultats obtenus pour

---

976 CHEMINAT (J.), « L'accès au code source d'un logiciel d'analyse d'ADN à la barre », *Le Monde Informatique*, 5 février 2021 [en ligne].

977 Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 52.

978 Exemple de définition :« La valeur p est la probabilité d'obtenir un effet égal ou plus extrême que celui observé en supposant que l'hypothèse nulle d'absence d'effet est vraie ; elle donne aux chercheurs une mesure de la force de la preuve contre l'hypothèse nulle » extrait traduit issu de BIAU (D-J.), JOLLES (B.M.) and PORCHER (R.), "P Value and the Theory of Hypothesis Testing: An Explanation for New Researchers", *Clin Orthop Relat Res* 468(3), 2010, pp. 885–892 [en ligne].

979 McCABE (D.), "NOVA : Prediction by the Numbers", *op. cit.*

qu'ils répondent aux attentes des chercheurs, ce que certains n'hésitent pas à faire afin de pouvoir publier des articles scientifiques sur le sujet.

382. En outre, l'enjeu portant sur les erreurs décisionnelles liées à l'utilisation d'un algorithme ne se limite pas aux seuls concepteurs mais également aux utilisateurs de l'algorithme qui développent une tendance à se fier aveuglément aux résultats fournis, qu'ils estiment comme nécessairement rigoureux et fiables. Dès lors, en accordant une confiance disproportionnée aux résultats produits par les algorithmes, les utilisateurs prennent des décisions erronées. Aussi, les algorithmes effectuent des calculs de probabilités qui même lorsqu'ils sont élevés (avoisinant les 100%) ne constituent pas pour autant une affirmation[980]. L'usage d'algorithmes d'aide à la prise de décisions en matière pénale, notamment à des fins de preuve, pourrait ne pas convenir du seul fait qu'ils produisent des résultats avec un certain degré de certitude qui n'en n'est pas pour autant une affirmation.

383. Le Parlement européen émettait ainsi des réserves à l'égard du recours systématique à des algorithmes par les services répressifs, estimant que « même avec un faible taux de faux positifs, [ceux-ci peuvent] entrainer bien plus de fausses alertes que de vrais alertes »[981]. Le manque de fiabilité de cette technologie pourrait, d'une part, perturber l'action des forces de l'ordre et, d'autre part, porter atteinte aux droits et libertés des individus faisant l'objet d'une décision reposant partiellement sur un tel algorithme. Cette insuffisance de fiabilité peut notamment résulter de différentes formes de biais algorithmiques.

B. Les biais algorithmiques des technologies de surveillance de sécurité publique

384. Aujourd'hui, un des enjeux principaux concernant le recours à l'IA portent sur les biais algorithmiques de programmation auxquels sont confrontés les modèles d'apprentissage machine. Outre les attentes en matière d'efficacité, les algorithmes sont supposés fournir des résultats neutres exemptés des préjugés et des biais dont peuvent être affectés les êtres humains[982]. Or, un algorithme effectue ses calculs à partir des données qui lui ont été fournies et en suivant un modèle prédéfini

[980] LELIEUR (J.), « L'intelligence artificielle : une nouvelle technologie probatoire en émergence », *op. cit.*

[981] Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*, cons. M.

[982] DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020 [en ligne].

par ses concepteurs, par conséquent il ne peut être automatiquement neutre[983]. Le terme de neutralité n'est au demeurant pas des plus adéquat et celui de loyauté lui est donc souvent préféré[984]. La loyauté algorithmique repose sur le fait pour un algorithme de produire des résultats conformes aux attentes. Au-delà de la loyauté, les principes juridiques et éthiques en matière de non-discrimination exigent l'équité des algorithmes[985]. En d'autres termes, il s'agirait pour ces algorithmes de ne pas produire de résultats effectuant une distinction entre les personnes qui reposerait sur les critères énoncés par le Code pénal[986] tels que l'origine ethnique ou encore le genre[987].

385. Un algorithme peut engendrer des résultats aberrants du fait de biais qui peuvent conduire à créer ou renforcer une discrimination à l'égard de certaines personnes ou catégories de personnes[988]. Bien que les effets discriminants de l'IA soient étroitement liés aux biais algorithmiques, les biais ne sont pas toujours à l'origine de discriminations[989]. Il convient donc de bien distinguer la notion de biais de celle de discrimination[990]. Le terme « biais » peut avoir différentes significations en fonction du contexte ainsi que du domaine pour lequel un algorithme est utilisé. Les biais peuvent être cognitifs (humains), statistiques, économiques, différentiels ou

---

983 *Idem* : « En réalité, […] les algorithmes sont conçus par des êtres humains et à partir de données reflétant des pratiques humaines. Ce faisant des biais peuvent être ainsi intégrés à toutes les étapes de l'élaboration et du déploiement des systèmes ». Voir également en ce sens : BAROCAS (S.) and SELBST (A.D.), "Big Data's disparate impact", *California Law Review* n° 3, Vol. 104, June 2016, pp. 671-732 [en ligne].

984 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*

985 Un algorithme est qualifié d'équitable lorsque ses résultats ne produisent pas un effet discriminant ou de biais à l'encontre d'une catégorie spécifique de personnes (PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *op. cit.*, p. 6). CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 113-118 ; DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », *op cit.*

986 CP, art. 225-1 à 225-4.

987 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 213 ; BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*

988 European Union Agency for Fundamental Rights (FRA), Report on "Bias in algorithms - artificial Intelligence and Discrimination", Vienna, December 8th 2022, p. 22 [en ligne] ; LELIEUR (J.), « L'intelligence artificielle : une nouvelle technologie probatoire en émergence », *op. cit.* ; CNIL, « Comment remettre à l'Homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.*, p. 32.

989 PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

990 FRA, Report on "Bias in algorithms - artificial Intelligence and Discrimination", *op. cit.*, p. 22.

encore correspondre à un paramètre d'estimation[991]. Deux types de biais sont particulièrement susceptibles d'affecter des algorithmes d'analyse d'images issus de caméras de vidéoprotection : les biais cognitifs et les biais statistiques (1). Or, ces biais sont susceptibles d'engendrer des résultats allant à l'encontre du principe d'égalité et de non-discrimination (2).

1. Les principaux biais affectant les algorithmes d'analyse d'images

386. Les algorithmes produisent leurs résultats à partir d'une formule mathématique, des données d'apprentissage (introduites par leurs concepteurs) et des données collectées par leurs utilisateurs. Dès lors, les résultats des algorithmes reposent principalement sur la manière dont les programmeurs ont conçus ces algorithmes. Or, des recherches publiées en psychologie et en sciences cognitives démontrent que tous les êtres humains sont sujets à des biais cognitifs lorsqu'ils sont amenés à prendre des décisions[992]. Dès lors, ces biais cognitifs peuvent être également reproduits dans la conception des algorithmes de manière consciente ou inconsciente.

387. Les biais cognitifs - Les biais cognitifs peuvent être définis comme « une distorsion de la manière dont l'information est traitée par rapport à un comportement rationnel ou à la réalité »[993]. En psychologie cognitive, ils peuvent également être définis comme « un schéma de pensée trompeur et faussement logique » qui conduit à produire un raisonnement erroné résultant d'une tentative de résolution d'un problème sans disposer de connaissances suffisantes, qui simplifie la réalité[994]. De manière plus sommaire, la mathématicienne Cathy O'Neil qualifie les biais cognitifs comme étant « un ensemble d'opinions dissimulées dans des codes mathématiques »[995]. Un des

---

991 En apprentissage profond (*deep learning*), le terme biais est aussi utilisé pour désigner un paramètre d'estimation. Cette signification technique est uniquement utilisée dans le domaine informatique de l'apprentissage machine [FRA, Report on "Bias in algorithms - artificial Intelligence and Discrimination", *op. cit.*, p. 23]. Cette signification n'étant pas pertinente dans la discussion, elle ne sera pas prise en compte dans cette étude.

992 ALLAIS (M.), « Le comportement de l'homme rationnel devant le risque : critiques des postulats et axiomes de l'école Américaine », *Econometrica* n°4, vol. 21, 1953, pp. 503-546 ; KAHNEMAN (D.), SLOVIC (P.) and TVERSKY (A.), "Judgment under Uncertainty: Heuristics and Biases", *Science*, New Series n° 185, 1974, pp. 1124-1131 ; FREDERICK (S.), "Cognitive reflection and decision making", *Journal of Economic Perspectives* n°4, vol. 19, 2005, pp. 25-42.

993 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*

994 ISOARD (G.), « Algorithmes et biais cognitifs », p. 90 *in* DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, *op. cit.*

995 O'NEIL (C.), *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy*, New York, Crown Publishers, First edition, 2016, 209 p. [en ligne]. Voir aussi : O'NEIL (C.), *Algorithmes, la bombe à retardement*, Paris, Éditions Les Arènes, 2018, 340 p.

biais cognitifs les plus susceptibles de renforcer les discriminations est celui de stéréotype où l'attitude d'un individu correspond à celle de référence qui est généralement attribuée au groupe social auquel il s'identifie plutôt qu'à ses capacités individuelles[996]. Plusieurs publications scientifiques font état de l'existence des biais de stéréotype[997] qui ont pour conséquence de créer une forme d'auto-censure des personnes issues de certains groupes sociaux qui pensent être jugées sur la base de ces stéréotypes plutôt que sur leurs véritables personnalité et compétences. Aussi, d'autres facteurs, extérieurs cette fois, peuvent venir influencer le programmeur de l'algorithme tels que des méthodes très usitées dont l'exactitude scientifique n'a pourtant pas été vérifiée. Des résultats issus d'expériences similaires peuvent également induire des biais d'anticipation et de confirmation[998].

388. D'une manière générale, ces biais sont involontaires et peuvent ne pas être uniquement imputés aux seuls actes des concepteurs des algorithmes « augmentés ». De fait, l'apprentissage des algorithmes « augmentés » d'analyse d'images repose sur l'association d'un très grand nombre d'images à des mots ou à des catégories de situations. Compte tenu de la masse d'images à classifier, les concepteurs ont parfois recours à des personnes extérieures[999] qui peuvent elles aussi être sujettes à des biais cognitifs, comme tout être humain. En outre, ces dernières n'auront pas nécessairement la même perception de ces images dans leur travail de classification voire même ne percevront pas les conséquences de leur travail du fait de l'opacité des finalités de celui-ci.

389. Les biais statistiques - Les biais statistiques (ou biais liés aux données) reposent quant à eux sur la quantité, la qualité ou encore la pertinence des données utilisées. Un premier type de biais

---

996 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 10.

997 BLOCK (C. J.), KOCH (S.M.), LIBERMAN (B.E.), MERRIWEATHER (T.J.) and ROBERSON (L.) "Contending With Stereotype Threat at Work: A Model of Long-Term Responses", *The Counseling Psychologist* n°39, Vol.4, 2011, pp. 570-600 ; BOLUKBASI (T.), CHANG (K-W.), ZOU (J.), SALIGRAMA (V.) and KALAI (A.), "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", 30th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain, 2016.

998 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 10.

999 Sur ce sujet, le documentaire intitulé « Algorithmes - Vers un monde manipulé » décrit la manière dont procèdent certaines entreprises qui développent des algorithmes d'analyse d'images pour effectuer leur apprentissage par classement. Des témoignages démontrent que certains classements d'images sont effectués par des personnes extérieures à l'entreprise qui conçoit ces algorithmes. Celles-ci sont souvent peu rémunérées (mais leur situation sociale les contraint à accepter ce type de contrats par facilité du gain) ou soumises au travail forcé. Les personnes alors chargées de classifier ces images - en fonction de catégories préétablies - n'ont, le plus souvent, aucune connaissance des finalités pour lesquelles elles exécutent ces tâches (ARTE, « Algorithmes - Vers un monde manipulé », *arte.tv*, 2022, diffusé le 11 avril 2023).

statistique concerne les données qui peuvent être biaisées, inexactes ou approximatives. L'autre catégorie concerne des biais propres au domaine de la statistique[1000] tels que l'omission de variables déterminantes, la sélection des données inadéquates ou encore le biais d'endogénéité[1001]. Les biais peuvent avoir différentes origines. En premier lieu, ils peuvent provenir d'un sur-apprentissage où les paramètres du modèle mathématique fournissent des résultats concluants avec le jeu de données d'apprentissage mais pas avec d'autres types de données[1002]. Les chercheurs en apprentissage machine semblent néanmoins être parvenus à pallier cette difficulté par l'intermédiaire d'outils de validation croisée[1003].

390. En deuxième lieu, les biais peuvent provenir directement des données d'apprentissage couramment désigné par l'acronyme anglo-saxon GIGO pour *garbage in garbage out*[1004] faisant référence au fait que en dépit d'un modèle d'algorithme fonctionnel celui-ci produira des résultats inexacts si les données d'entrée sur lesquelles il aura été entrainé sont inexactes[1005]. Les données d'apprentissage peuvent être déséquilibrées par une sur-représentation de certains groupes (ex. adultes par rapport à des enfants) ou encore être erronées par un outil défaillant ou aux performances insuffisantes (ex. images d'une caméra dysfonctionnelle). Ce type de biais soulève d'importants enjeux en ce qu'il donne l'illusion de fournir des résultats satisfaisants alors que ceux-ci sont erronés. Ce biais des données peut en outre provenir de biais cognitifs.

391. En dernier lieu, les biais peuvent résulter du choix du modèle. Les modèles algorithmiques reposent sur différentes variables dont certaines s'avèrent difficiles à codifier car elles relèvent d'aspects assez subjectifs liés à l'être humain tels que les compétences humaines (*softs skills*). Or, le fait d'omettre certaines variables peut entacher la fiabilité des résultats de

---

1000 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 10.

1001 Les algorithmes reposent fréquemment sur des données passées afin de donner une estimation des évènements futurs. Or, il semblerait que l'anticipation des comportements humains ne soient pas (encore) possible à l'échelle d'un algorithme.

1002 PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

1003 *Idem*, note de bas de page 7 : « La validation croisée consiste à subdiviser les observations d'entrée et de sortie disponibles en un sous-groupe d'observation pour apprendre le modèle et en un sous-groupe d'observation pour tester si le modèle appris fait des prédictions qui se généralisent bien à des données différentes de celles d'apprentissage ».

1004 Qui pourrait se traduire par « les erreurs en entrée se retrouvent en sortie ».

1005 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 10 ; PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

l'algorithme voire engendrer des discriminations[1006]. De manière assez similaire, le biais de sélection apparait lorsque les caractéristiques des personnes ayant servies de données d'apprentissage ne correspondent pas à celles de la population générale. Il peut aussi résulter de données manquantes sur un ou plusieurs individus.

392. Les effets sur la fiabilité des algorithmes - Enfin, la fiabilité des algorithmes pâtit d'une insuffisance d'études indépendantes conduites en matière d'évaluation de l'efficacité réelle, sur le terrain, des algorithmes d'analyse d'images vidéo destinés à l'usage des forces de l'ordre. Les rares études publiées sur le sujet visant à mesurer l'incidence du recours à des algorithmes à des fins de sécurité publique ne sont pas véritablement concluantes[1007]. Aussi, il convient de garder à l'esprit qu'aucun algorithme n'est exempt de biais[1008] et que leurs résultats comprendront invariablement une marge d'erreurs. En ce sens, le Sénat déclarait que « la question de la fiabilité des algorithmes ne relève pas uniquement de leurs performances intrinsèques, mais également du seuil de correspondance souhaité et du taux d'erreurs toléré pour chaque cas d'usage »[1009].

393. Le seuil d'acceptabilité du taux d'erreurs de l'algorithme devrait correspondre à des niveaux d'exigence différents selon que l'algorithme soit chargé d'analyser des DACP ou non et plus particulièrement s'agissant de potentielles analyses de données biométriques. L'insuffisante fiabilité des algorithmes d'analyse d'images de vidéoprotection engendre des conséquences plus ou moins graves sur l'activité des forces de l'ordre ainsi que sur les droits et libertés des personnes. À titre principal, le manque de fiabilité d'un algorithme peut conduire à des discriminations ; en d'autres termes un algorithme peut porter atteinte au principe d'égalité et de non-discrimination.

1006 ZLIOBAITE (I.) and CUSTERS (B.), "Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models", *Artificial Intelligence and Law* (24), October 7th 2016, pp. 183-201 [en ligne] ; KLEINBERG (J.) and *al.*, "Human Decisions and Machine Predictions", *The Quarterly Journal of Economics*, Oxford University Press, vol. 133(1), 2018, pp. 237-293 [en ligne] ; MORIN-MARTEL (A.), "Machine learning in bail decisions and judges' trustworthiness", *AI &* Soc, April 21st 2023 [en ligne].

1007 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 72.

1008 En ce sens, la CNIL affirmait que « tout algorithme est, en un sens, biaisé, dans la mesure où il est toujours le reflet – à travers son paramétrage et ses critères de fonctionnement, ou à travers les données d'apprentissage qui lui ont été fournies – d'un système de valeurs et de choix de société » (CNIL, « Comment permettre à l'homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.*, p. 31 [en ligne]).

1009 Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 60.

2. Les biais algorithmiques facteurs d'inégalité et de discrimination

394. Les principes d'égalité et de non-discrimination - L'égalité juridique des individus est l'un des principes intangibles énoncés par la DDHC[1010] et est une égalité de droit qui « exige que toutes les personnes placées dans des situations identiques soient soumises au même régime juridique, soient traitées de la même façon, sans privilège et sans discrimination »[1011]. En outre, le principe d'égalité devant la loi est consacré au sein du bloc de constitutionnalité français[1012]. Il implique que le droit ne fasse pas de distinction entre les personnes. Néanmoins, la formule énonçant que « la loi doit être la même pour tous » ne s'applique que dans le cas où les personnes sont placées dans des situations identiques. Dès lors, le principe d'égalité « ne s'oppose pas à ce que le législateur traite différemment des personnes ou des groupes de personnes placées dans des situations différentes »[1013]. Ces affirmations ont été formulées et confirmées par le juge administratif[1014]. Dans le même sens, le Conseil constitutionnel affirme de manière constante depuis sa décision du 12 juillet 1979[1015] que « le principe d'égalité ne s'oppose ni à ce que le législateur règle de façon différente des situations différentes, ni à ce qu'il déroge à l'égalité pour des raisons d'intérêt général pourvu que, dans l'un et l'autre cas, la différence de traitement qui en résulte soit en rapport direct avec l'objet de la loi qui l'établit »[1016].

[1010] DDHC, art 1er : « Les hommes naissent et demeurent libres et égaux en droits ».

[1011] ODENT (R.), *Contentieux administratif*, Tome II, Paris, Dalloz, 2007, 783 p., p. 353.

[1012] DDHC, art. 1er, 6 et 13 ; Constitution de 1946, Préambule al. 3 : « La loi garantie à la femme, dans tous les domaines, des droits égaux à ceux de l'homme » ; Constitution de 1958, art. 1er : « La France est une République indivisible, laïque, démocratique et sociale. Elle assure l'égalité devant la loi de tous les citoyens sans distinction d'origine, de race ou de religion ». Le Conseil constitutionnel confère au principe d'égalité une valeur constitutionnelle depuis sa décision du 27 décembre 1973 (C. const., Décision n° 73-51 DC, 27 décembre 1973, *Loi de finances pour 1974*, Rec. p. 25, cons. 2 [en ligne]).

[1013] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, pp. 630-631.

[1014] CE, sect., 10 mai 1974, n° 88032, *Denoyez et Chorques* [en ligne] ; CE, ass., 11 avril 2012, n° 322326, *op. cit.* : « le principe d'égalité ne s'oppose pas à ce que l'autorité investie du pouvoir réglementaire règle de façon différente des situations différentes ni à ce qu'elle déroge à l'égalité pour des raisons d'intérêt général pourvu que, dans l'un comme dans l'autre cas, la différence de traitement qui en résulte soit en rapport direct avec l'objet de la norme qui l'établit et ne soit pas manifestement disproportionnée au regard des motifs susceptibles de la justifier ».

[1015] C. const., Décision n° 79-107 DC, 12 juillet 1979, *Loi relative à certains ouvrages reliant les voies nationales ou départementales*, Rec. p. 31, cons. 4 [en ligne].

[1016] C. const., Décision n° 2009-578 DC, 18 mars 2009, *Loi de mobilisation pour le logement et la lutte contre l'exclusion*, Rec. p. 73, cons. 19 [en ligne]. Voir aussi : C. const., Décision n° 96-380 DC, 23 juillet 1996, *Loi relative à l'entreprise nationale France télécom* [en ligne] ; C. const., Décision n° 97-388 DC, 20 mars 1997, *Loi créant les plans d'épargne retraite*, Rec. p. 31, cons. 27 [en ligne].

395. Ce principe est également affirmé par de nombreux textes internationaux[1017] et par la jurisprudence européenne. Les juges européens adoptent une position plus stricte que les juges nationaux en ce qu'ils estiment que « le principe d'égalité veut que des situations comparables ne soient pas traitées de manière différente et que des situations différentes ne soient pas traitées de manière égale »[1018]. En ce sens, les juges européens instaurent une obligation de traiter différemment des personnes dans des situations différentes.

396. Le principe de non-discrimination, principe corollaire au principe d'égalité, est consacré tant par les textes internationaux[1019] que nationaux[1020]. Ce principe est affirmé par les juridictions nationales[1021] et supranationales[1022]. Bien qu'ils soient souvent confondus, les principes d'égalité et de non-discrimination ont une signification différente. Le principe de non-discrimination entend principalement interdire l'utilisation de critères, considérés comme illégitimes, en vue d'aboutir à des situations différentes. En d'autres termes, ce principe impose de faire abstraction des différences entre les individus[1023]. À l'inverse, le principe d'égalité permet la création de catégories différentes à des fins légitimes[1024]. Dès lors, le respect des principes d'égalité et de non-discrimination suppose l'adoption de critères objectifs et rationnels en accord avec la réglementation. Il exige également que les différences de traitement soient adaptées et proportionnées aux finalités poursuivies.

[1017] DUDH, art. 2 ; CDFUE, art. 20 ; Conv.EDH, art. 14 et Protocole n° 12, art. 1er.

[1018] De manière non-exhaustive : CJCE, 13 novembre 1984, *Racke v. Hauptzollamt Mainz*, aff. C-283/83 [en ligne] ; CEDH, 6 avril 2000, *Thlimennos c. Grèce*, n° 34369/97 [en ligne] ; CJCE, gr. ch., 16 décembre 2008, *Arcelor*, aff. C-127/07, pt. 23 [en ligne] ; CEDH, 30 juin 2016, *Taddeucci et McCall c. Italie*, n° 51362/09 [en ligne].

[1019] CDFUE, art. 21, al. 1er ; Conv.EDH, art. 14 : « la jouissance des droits et libertés reconnus […] doit être assurée sans distinction aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation » ; TFUE, art. 18 et 19 ; Pacte international relatif aux droits civils et politiques (PIDCP), art. 26.

[1020] Constitution de 1946, Préambule al. 1er.

[1021] C. const., Décision n° 2007-557 DC, 15 novembre 2007, *Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile*, Rec. p. 360, cons. 29 [en ligne] : Le juge constitutionnel avait censuré la loi au motif qu'elle contrevenait à l'article 1er de la Constitution.

[1022] CJCE, 8 avril 1976, *Defrenne c. Belgique*, aff. C-43/75, spéc. pt. 16 [en ligne] : Le juge européen consacre le principe de non-discrimination (fondé sur le sexe) comme principe général du droit communautaire.

[1023] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 437.

[1024] BIOY (X.), « Droit constitutionnel », (46-47-11), p. 404 *in* BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, Paris, Dalloz, 3ème édition, 2021, 943 p. ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 635.

397. Les effets d'une insuffisante fiabilité des algorithmes - Les algorithmes d'analyse d'images de drones aériens de sécurité publique à des fins de détection de comportement anormaux sont susceptibles de contenir des biais qui entachent la fiabilité de leurs résultats. Ils pourraient même amplifier ce phénomène de biais par l'automatisation voire produire des résultats pouvant être considérés comme attentatoires au principe d'égalité et de non-discrimination. La loi du 27 mai 2008 relative à la lutte contre les discriminations comporte une définition large de la notion comme étant « tout agissement […] subi par une personne et ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile dégradant, humiliant ou offensant »[1025]. Elle distingue deux formes de discrimination : la discrimination directe et la discrimination indirecte[1026]. La discrimination peut être qualifiée si deux critères sont remplis à savoir celui d'effectuer une distinction, d'une part, et le fait de fonder cette distinction sur un ou des critères illégaux, d'autre part. Ainsi, le fait d'« isoler » un individu au sein d'une foule au motif que son comportement est considéré comme « anormal » par l'algorithme pourrait être assimilable à une forme de discrimination si les critères qualifiant l'individu d' « anormal » sont illégaux ou s'ils s'avéraient inexplicables[1027].

398. La fiabilité des algorithmes « augmentés » associés aux drones aériens de sécurité publique est un enjeu crucial tant s'agissant des activités des forces de l'ordre que du respect des droits et libertés des personnes concernées par le traitement des données. L'absence de fiabilité des données tout comme celle de l'algorithme pourrait avoir de graves conséquences pour les individus dans le cadre d'une procédure pénale. Aussi, la fiabilité des données n'est pas la seule condition au respect des principes relatifs à la procédure pénale. Face à la complexité des algorithmes « augmentés », les utilisateurs mais aussi les concepteurs sont confrontés à des difficultés s'agissant de donner des explications claires quant à leur mode de fonctionnement. Cette difficulté s'oppose

---

[1025] Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations, *JORF* n°0123 du 28 mai 2008 [en ligne].

[1026] *Idem*, art. 1er, al. 2 : Est considéré comme constitutif d'une discrimination indirecte « une disposition, un critère ou une pratique neutre en apparence (nous soulignons), mais susceptible d'entraîner […] un désavantage particulier pour des personnes par rapport à d'autres personnes, à moins que cette disposition, ce critère ou cette pratique ne soit objectivement justifié par un but légitime et que les moyens pour réaliser ce but ne soient nécessaires et appropriés ».

[1027] En ce sens Caroline Lequesne Roth s'inquiétait de la forte probabilité de voir apparaitre des discriminations lorsqu'une analyse comportementale est effectuée par des caméras, y compris lorsqu'elles n'effectuent pas de réidentification d'individus et qu'elles se focalisent sur la foule plutôt que sur les individus pris individuellement. À titre d'exemple, elle soulevait l'enjeu que posait les personnes autistes déclarant qu'*in fine* « on ne sait pas ce qu'est un comportement "normal" » (BERTRAND (B.), « Encadrement des technologies de surveillance : les enseignements de l'expérimentation des JO 2024 », 22 mars 2023 [Visioconférence en ligne]).

pourtant à leur « acceptabilité » dans un sens général ainsi que dans le cadre des opérations des forces de l'ordre et éventuellement d'une procédure pénale.

§2. L'opacité entourant les algorithmes « augmentés » facteur d'insécurité juridique

399. L'opacité d'un algorithme « fait référence au niveau de compréhension de sa logique »[1028] par ses utilisateurs. Les algorithmes sont parfois qualifiés de « boîtes noires » (*black boxes*) tant par les médias que par les scientifiques du domaine dont le mathématicien Cédric Villani[1029]. Cette qualification fait référence au fait que les personnes qui font usage ou sont directement concernées par les résultats, plus ou moins satisfaisants, d'un algorithme n'ont pas connaissance de son mode de fonctionnement. En d'autres termes, le fonctionnement des algorithmes basés sur l'apprentissage machine peut toujours comporter une part d'inexplicable[1030]. S'agissant d'autres types d'algorithmes, certains concepteurs sont en mesure d'interpréter leur raisonnement et d'en expliquer le fonctionnement (*white box AI*).

400. Avant d'entrer plus précisément dans le sujet, il convient de préciser que par opacité il faut ici entendre une carence en matière d'explicabilité des algorithmes, d'une part, et de transparence du recours à ces algorithmes, d'autre part. Le fait est que, s'agissant des algorithmes, les termes d' « explicabilité » et de « transparence » sont fréquemment employés comme synonymes. Pourtant, les deux termes désignent des objectifs distincts. Les principes d'explicabilité et de transparence sont étroitement liés mais ne doivent pas être confondus[1031]. La transparence traduit le fait qu'une information ait été transmise à toute personne intéressée concernant les activités d'une personne privée ou publique (selon le principe de loyauté)[1032]. Elle supposerait aussi

---

[1028] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 215.

[1029] Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.* ; PASQUALE (F.), *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, MA: Harvard University Press, 2015 ; MEILLER (Y.), « Intelligence artificielle, sécurité et sûreté », *Sécurité et stratégie* n° 28, janvier 2018, pp. 75-84, spec. p. 81 [en ligne].

[1030] Les algorithmes d'IA sont regroupés au sein deux catégories : explicite ou implicite. Les algorithmes explicites reposent sur une logique entièrement conçue par des êtres humains et sont, pour la plupart, explicables. À l'inverse, les algorithmes implicites reposent sur une logique construite à partir d'un apprentissage machine où l'algorithme est entrainé sur un jeu de données. Ces derniers font le plus fréquemment l'objet de calcul d'explicabilité.

[1031] JEAN (A.), « Transparence et explicabilité des algorithmes, la grande confusion », *lepoint.fr*, 13 juin 2021 [en ligne] : transparence et explicabilité des algorithmes « deux concepts qu'il ne faut pourtant pas confondre […] Ces deux mots s'entremêlent avec maladresse, alors que l'un n'implique pas l'autre, et *vice versa* ».

[1032] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, pp. 204-205 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 265 ; JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 212.

que l'algorithme soit équitable. Néanmoins, il parait nécessaire de préciser que dans le cas de l'usage d'algorithmes par une autorité publique cela n'induit pas nécessairement que celle-ci communique la formule mathématique des algorithmes mais qu'elle informe les personnes concernées de leur usage et de la manière dont il fonctionne.

401. D'une manière générale, un algorithme est reconnu comme étant explicable « s'il est possible de donner à l'ensemble des utilisateurs, quel que soit leur bagage éducatif, une vision claire des procédures employées et des fonctionnalités remplies par l'algorithme, afin de permettre un usage informé »[1033]. L'explicabilité constitue un enjeu général puisqu'il concerne toute personne susceptible d'être concernée par l'utilisation d'un algorithme, indépendamment de ses compétences. Il s'agit notamment d'un enjeu crucial en matière de décision des pouvoirs publics où l'opacité du fonctionnement de l'algorithme, de par sa complexité, pourrait être légitimement contestée par toutes personnes concernées[1034]. L'explicabilité est une discipline du domaine des algorithmes qui consiste à élaborer des méthodes numériques permettant d'extraire la logique de fonctionnement d'un algorithme. De fait, il est fréquent dans le domaine de l'apprentissage machine que les concepteurs de modèles d'algorithmes ne soient pas en mesure d'expliquer entièrement leur apprentissage ou leur fonctionnement. En outre, il n'existe aujourd'hui aucune technique standardisée permettant de formuler une requête à l'algorithme d'expliciter son processus de « raisonnement » l'ayant amené à rendre ses résultats[1035]. L'explicabilité est pourtant un élément intrinsèque de l'algorithme. Elle suppose de fournir des éléments de réponse sur le fonctionnement de l'algorithme aux personnes concernées. Cette condition pose néanmoins des difficultés d'ordre pratique quant au discours à adopter (aussi désigné comme « la pédagogie des algorithmes »). En ce sens, deux solutions d'explicabilité sont envisageables. La première solution consiste à adapter l'explicabilité au public visé permettant d'assurer le respect des droits de toute personne concernée. La deuxième solution serait de soumettre une seule forme d'explicabilité par algorithme dans un souci de clarté[1036].

[1033] PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *op. cit.*, p. 7.

[1034] *Idem*.

[1035] Voir en ce sens : KNIGHT (W.). "The Dark Secret at the Heart of IA", *The MIT Technological Review*, 120 (3), 2017.

[1036] Ainsi, « la prolifération de représentations diverses d'un même algorithme pourrait poser des problèmes graves de communication, voire de responsabilité légale » (PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *op. cit.*, p. 8).

402. Le fait est que les enjeux relatifs à l'opacité des algorithmes d'IA ne se limitent pas aux seuls utilisateurs. En ce sens, les forces de l'ordre ayant recours à des outils algorithmiques devront en maitriser le fonctionnement mais les personnes concernées par leurs traitements sont également légitimes à connaître leur fonctionnement. Or, certaines études font état des inégalités numériques en France au sein du grand public[1037]. Outre les difficultés d'accès aux outils numériques, la question de leur maitrise constitue probablement l'enjeu principal de ces inégalités. Aussi, à mesure que les progrès technologiques s'intensifient, les non-spécialistes (par opposition aux personnes qui développent et maitrisent les algorithmes « augmentés ») sont de moins en moins en mesure de comprendre la terminologie et le fonctionnement des avancées technologiques issues du domaine des algorithmes d'IA[1038]. Pire, les forces de l'ordre pourraient également être dépassées par la technique[1039] et nécessiteront une formation leur permettant d'assurer une certaine maitrise de ces outils[1040].

403. Indépendamment des utilisateurs, ce sont les concepteurs eux-mêmes qui peuvent se trouver parfois confrontés à un manque d'explicabilité d'un ou de plusieurs algorithmes[1041]. Le terme « intelligibilité » sera alors plus fréquemment employé dans ce cas car il fait référence au fait pour les concepteurs d'être en mesure de comprendre le fonctionnement d'un algorithme et d'examiner si celui-ci répond effectivement aux conditions souhaitées. Dès lors, l'intelligibilité est étroitement liée à l'explicabilité des algorithmes puisque, de fait, la compréhension est l'étape préalable nécessaire à l'explication. L'intelligibilité des algorithmes est donc reconnue comme un enjeu majeur en l'informatique et constitue un des axes de recherche principaux du domaine, au

---

[1037] Selon le rapport du Conseil d'État du 31 mars 2022 : « l'illectronisme (ou illettrisme numérique) touche 17% de la population : une personne sur six n'utilise pas Internet, une personne sur quatre ne sait pas s'informer *via* Internet, et une personne sur cinq est incapable de communiquer sur ce réseau » (p. 49). Voir en ce sens : INSEE Première, n° 1780, 30 octobre 2019 [en ligne].

[1038] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 48 ; IFOP, « Notoriété et image de l'intelligence artificielle auprès des Français et des salariés », *ifop.com*, 28 janvier 2021 [en ligne]. Voir sur le sujet : BURRELL (J.), "How the machine "thinks" : Understanding opacity n machine learning algorithms", *Big Data Society*, 2016 p. 4 ; BRIGGS (E.), "The AI Frenzy Is Introducing Marketing Buzzwords That Consumers Don't Understand", *Morning Consult*, April 24th 2023 [en ligne] consulté le 11 mai 2023.

[1039] Voir en ce sens une étude publié par l'Université de Caroline du Nord aux États-Unis : DEMPSEY (R.P.), BRUNET (J.R.) and DUBLJEVIĆ (V.), "Exploring and Understanding Law Enforcement's Relationship with Technology: A Qualitative Interview Study of Police Officers in North Carolina", *Applied Sciences*, March 18th 2023 [en ligne] ; « Les outils d'IA sont utilisés par la police qui ne comprend pas comment ces technologies fonctionnent », selon une étude de l'Université d'État de Caroline du Nord », *développez.com*, 17 mai 2023 [en ligne] consulté le 17 mai 2023.

[1040] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 50.

[1041] Il peut s'agir de limites issues de l'état de l'art scientifique ou à des limites scientifiques plus générales.

même titre que l'explicabilité[1042]. Aussi, l'intelligibilité et l'explicabilité des algorithmes sont intrinsèques à la transparence (avec la loyauté et l'équité) puisque de fait cette dernière nécessite que le concepteur soit en mesure de comprendre, de maitriser et d'expliquer leur fonctionnement.

404. Ainsi que l'affirme le Conseil d'État : « l'opacité est destructrice de confiance »[1043]. Le seul fait d'avoir recours, y compris de manière légitime, à des algorithmes d'analyse d'images de drones aériens de sécurité publique sans que les personnes concernées puissent en discerner l'existence et le fonctionnement peut susciter des réactions d'hostilité. Les pouvoirs publics doivent par conséquent respecter un principe de loyauté dans l'utilisation de cette technologie au même titre que tout autre système de traitement de données en vertu des dispositions relatives à l'emploi de drones aériens de sécurité publique[1044] ainsi que de celles relatives à la protection des DACP[1045]. Aussi, les autorités publiques ayant recours à des technologies reposant sur de l'IA doivent faire face à des enjeux majeurs en matière de sécurité informatique qui, souvent, dépassent ceux déjà répertoriés en matière d'outils connectés.

§3. Les cybermenaces propres aux algorithmes « augmentés »

405. Les usages des algorithmes « augmentés » sont multiples ; il est dès lors possible d'envisager diverses formes de détournement de leur utilisation. Ainsi, à l'instar de toute technologie connectée, les algorithmes « augmentés » associés aux drones aériens de sécurité publique sont susceptibles de faire l'objet d'une attaque informatique[1046] pouvant modifier leur fonctionnement et leur contenu. Le traitement d'images par un algorithme peut être sujet à une atteinte à sa sécurité lors que celui-ci fait l'objet d'une attaque informatique. Des chercheurs

---

[1042] Voir notamment : GUNNING (D.) and *al.*, "Explainable Artificial Intelligence (XAI)", *Science Robotics*, Vol. 4 (37), December 18th 2019 [en ligne] ; BARREDO ARRIETA (A.) and *al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI", *Information Fusion*, Vol. 58, June 2020, pp. 82-115 [en ligne] ; GOHEL (P.), SINGH (P.) and MOHANTY (M.), "Explainable AI: current status and future directions", *Computer Science*, July 12th 2021 [en ligne] ; KHAKUREL (U.) and RAWAT (D.B.), "Evaluating Explainable Artificial Intelligence: Algorithmic Explanations for Transparency and Trustworthiness", *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications IV*, Vol. 12113, June 6th 2022 [en ligne].

[1043] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 118.

[1044] CSI, art. 242-3 : « le public est informé par tout moyen approprié de l'emploi de dispositifs aéroportés de captation d'images ».

[1045] Le principe de loyauté du traitement de DACP est affirmé par la LIL (art. 4 §1), le RGPD (art. 5 §1a) et la DPJ (art. 4 §1 a).

[1046] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 126-127.

américains en cybersécurité ont notamment lancé une alerte au printemps 2021 sur un nouveau type d'attaque ciblant les SIA[1047] et, par conséquent, les algorithmes « augmentés ». À titre d'exemple, des chercheurs de l'université Carnegie Mellon sont parvenus à perfectionner une des techniques très en vogue, le *deepfake*[1048]*,* en créant des algorithmes capables de collecter une vidéo et d'appliquer son contenu sur une autre sans qu'il soit possible de déceler son altération à l'œil nu.

406. Outre les enjeux qu'elles présentent en termes de désinformation, les techniques d'altération du contenu d'une image ou d'une vidéo remettent en question l'intégrité même de celle-ci. En ce sens, des chercheurs se sont aperçus qu'il était possible à l'aide d'un algorithme de *deep fake* de modifier des informations telles que des images satellites[1049]. Le recours à des drones aériens « augmentés » de sécurité publique engendre deux types de vulnérabilité en cas d'attaque informatique ; l'une portant sur l'algorithme d'aide à la prise de décision et l'autre portant sur les enregistrements vidéo. Comme évoqué précédemment, les atteintes portées à l'intégrité des enregistrements vidéo entacheraient définitivement la validité de ceux-ci comme éléments de preuve au procès pénal. En revanche, les atteintes portées aux SAAD impliquent une nouvelle forme de menace en ce qu'elles ôtent toute forme de fiabilité de l'ensemble du système qu'il s'agisse des résultats présentés par les algorithmes autant que les données qu'ils traitent.

407. Les recherches scientifiques font état d'un ensemble étendu de types d'attaques pouvant être portées aux SIA[1050]. Le Laboratoire de la CNIL (LINC) classifie ces différentes typologies d'attaques en trois catégories selon le moment et l'objectif de celles-ci[1051] : les attaques par manipulation, les attaques par infection et les attaques par exfiltration. Ces attaques peuvent viser spécifiquement le SIA afin de porter directement atteinte à son fonctionnement ou encore en

---

1047 DELUZARCHE (C.), « Un nouveau type de cyberattaque qui fait bondir la consommation énergétique de l'IA », *Futura Sciences*, 11 mai 2021 [en ligne] consulté le 19 mai 2021 ; ROCHEFORT (M.), « Des chercheurs alertent sur une nouvelle forme de hack visant les IA », *Siècle Digital,* 7 mai 2021 [en ligne] consulté le 20 mai 2021.

1048 BANSAL (A.), MA (S.), RAMANAN (D.) and SHEIKH (Y.), "Recycle-GAN: Unsupervised Video Retargeting", *European Conference on Computer Vision* (ECCV), 2018 [en ligne].

1049 AUCLERT (F.), « Et si le « deepfake » contaminait les images satellites », *Futura Tech*, 23 avril 2021 [en ligne] ; ROCHERFORT (M.), « Des chercheurs alertent sur l'émergence des deepfakes d'images par satellite », *Siècle Digital*, 28 avril 2021 [en ligne] consultés le 30 avril 2021.

1050 VEALE (M.), BINNS (R.), EDWARDS (L.), "Algorithms that remember: model inversion attacks and data protection law", *Phil. Trans. R. Soc. A* 376, July 12th 2018, [en ligne].

1051 LINC, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *cnil.fr*, avril 2022 [en ligne] : Ce dossier publié par le laboratoire de la CNIL (LINC) porte sur la sécurité des SIA. Il comprend une description des types d'attaques dont ils peuvent faire l'objet ainsi que des solutions pouvant être mises en œuvre en amont afin de minimiser au mieux les potentialités d'atteinte.

détourner l'usage afin de dérober ses données. Aussi, les différents types d'attaques peuvent intervenir à différentes phases de l'algorithme : la phase d'apprentissage ou la phase de production (phase d'utilisation)[1052].

408. Les attaques par manipulation ont pour objectif de détourner les résultats de l'algorithme en injectant des données altérées en entrée afin de modifier le résultat de l'algorithme (données en sortie). Il s'agit d'une attaque visant à détourner un algorithme de ses finalités initiales au point, parfois, de le voir effectuer des tâches inattendues. Les attaques par manipulation peuvent être subdivisées en trois catégories d'attaques dont l'attaque par déni de service[1053] (*DDoS*). L'attaque par évasion est un des types d'attaque par manipulation. Elle consiste à introduire des données (images, son, texte, etc.) soigneusement modifiées en entrée qui ressemblent aux données d'entrée initiales de telle sorte à ce qu'un humain ne puisse pas s'en apercevoir mais que le système se trouve perturbé par ces « exemples contradictoires »[1054]. Ce type d'attaque s'inspire des difficultés auxquelles sont encore confrontés les algorithmes telles que les biais de sélection ou de surreprésentation. Ces attaques peuvent porter sur un large panel de SIA. L'attaque par reprogrammation est un autre type d'attaque par évasion qui consiste à dévier les finalités de l'algorithme afin de lui faire exécuter des tâches non initialement prévues. L'algorithme est reprogrammé à distance par l'attaquant par une introduction de données altérées en entrée[1055].

409. En matière d'algorithmes d'analyse d'images, les attaques portant sur la classification d'images pourraient avoir des effets particulièrement néfastes sur l'activité des forces de l'ordre. Les exemples contradictoires peuvent de fait modifier la reconnaissance des éléments sur une image

---

[1052] Les attaques par infection sont susceptibles d'apparaitre durant la phase d'apprentissage ; en d'autres termes, lorsque les concepteurs entrainent l'algorithme. Les attaques par manipulation peuvent se produire durant la phase de production, c'est à dire après la phase d'apprentissage. Les attaques par exfiltration ont la particularité de concerner autant la phase d'apprentissage que la phase de production (*Idem*, p. 9).

[1053] HONG (S.) *and al.*, "A Panda ? No, It's a Sloth : Slowdown Attacks on Adaptative Multi-Exit Neural Network Inference", *ICLR 2021*, February 25th 2021 [en ligne].

[1054] LINC, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *op. cit.*, p. 9. Voir aussi : GOODFELLOW (I.) *and al.*, "Generative Adversarial Nets", *NIPS'14: Proceedings of the 27th International Conference on Neural Information Processing Systems*, Vol. 2, December 2014, pp. 2672–2680 [en ligne] ; BIGGIO (B.) and ROLI (F.), "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning", *Pattern Recognition*, Vol. 84, December 2018, pp. 317-331 [en ligne].

[1055] Voir en ce sens : ELSAYED (G.F.), GOODFELLOW (I.) and SOHL-DICKSTEIN (J.), "Adversarial Reprogramming of Neuronal Network", November 29th 2018 [en ligne].

par l'algorithme donnant ainsi des résultats incohérents[1056]. Ce type d'attaque affecte principalement les algorithmes de classification d'images[1057]. Aussi, les attaques par exemples contradictoires pourraient affecter les drones aériens « augmentés » de sécurité publique lorsqu'ils ont pour finalités la détection de personnes[1058] ou encore la détection d'objets en temps réel[1059] voire plus spécifiquement la détection et la reconnaissance de panneaux routiers[1060]. En altérant les résultats par les données modifiées en entrée, l'algorithme est susceptible de déclencher inutilement des alertes ou, à l'inverse, d'empêcher le déclenchement d'alertes ôtant toute efficacité à l'algorithme supposé assister les forces de l'ordre dans le cadre de leurs missions. En outre, le détournement des finalités d'un algorithme porte atteinte aux droits et libertés des personnes dont principalement le droit à la protection de la vie privée et celui des DACP[1061]. Néanmoins, les chercheurs en informatique progressent dans leurs développements de solutions permettant de se protéger contre ce type d'attaques[1062].

410. Lors de la phase d'apprentissage, l'algorithme peut faire l'objet d'attaques par infection qui portent soit sur le fonctionnement du système (modification des labels ou étiquettes[1063], corruption logique[1064]) soit sur les données d'apprentissages (injection ou modification de

---

1056 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 126 : Le Conseil d'État soulignait l'existence d'attaque visant à leurrer l'algorithme et notait notamment que « la modification, imperceptible à l'œil nu d'un seul pixel sur une image peut ainsi entrainer une "prédiction" totalement différente et parfois aberrante ».

1057 Voir par exemple : GOODFELLOW (I.), SHLENS (J.) and SZEGEDY (C.), "Explaining and harnessing adversarial examples", *ICLR*, 2015 [en ligne] ; BROWN (T.) *and al.*, "Adversarial Patch", *31st Conference on Neural Information Processing Systems* (NIPS 2017), May 17th 2018 [en ligne].

1058 Voir notamment : YIN (M.) *and al.*, "ADC: Adversarial attacks against object Detection that evade Context consistency checks", *2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2022, pp. 2836-2845 [en ligne] ; JI (N.) *and al.*, "Adversarial YOLO: Defense Human Detection Patch Attacks via Detecting Adversarial Patches", March 16*th* 2021 [en ligne].

1059 WU (H.) *and al.*, "Adversarial Detection: Attacking Object Detection in Real Time", *IEEE Intelligent Vehicle Symposium, 2023*, May 31st 2023 [en ligne].

1060 EYKHOLT (K.) *and al.*, "Robust Physical-World Attacks on Deep Learning Visual Classification", *CVPR 2018*, April 10th 2018 [en ligne].

1061 Les dispositions relatives à la protection des DACP exigent que les finalités d'un traitement soient déterminées, légitimes et explicitées en amont de toute collecte (RGPD, art. 5 §1 b) ; DPJ, art. 4 §1 b), LIL, art. 4 §2). Dès lors, toute modification de ces finalités constitue une atteinte au droit à la protection des DACP et au droit à la vie privée.

1062 « Adversarial Attack : Définition et protection contre cette menace », *Datascientest*, 4 mars 2022 [en ligne].

1063 Système de marquage ou d'annotation des données notamment utilisé à des fins de classification de celles-ci.

1064 Modification de l'algorithme d'apprentissage.

données)[1065]. Il existe deux types d'attaques par infection : les attaques par empoisonnement[1066] et les attaques par portes dérobées (*backdoor attacks*). Les attaques par empoisonnement ont pour objectifs de détériorer la qualité des résultats d'un algorithme[1067]. Elles se distinguent des attaques par évasion dans le sens où la modification de données d'apprentissage permet d'altérer la structure du modèle de l'algorithme et non uniquement ses résultats. Cependant, les attaques par empoisonnement ne permettent pas aux utilisateurs malveillants d'avoir accès aux données initiales ni au modèle du SIA ; ils ne peuvent agir qu'en introduisant des données dans le modèle. À l'inverse, l'attaque par porte dérobée peut avoir des conséquences bien plus néfastes sur l'algorithme puisqu'elle permet à l'attaquant d'avoir accès au modèle du SIA et de le ré-entraîner à sa guise[1068]. Dès lors, les attaques par porte dérobée peuvent engendrer de graves effets sur les résultats du SIA et, de surcroit, peuvent persister lorsque d'autres modèles de SIA dont il est dérivé ont été infectés[1069].

411. Enfin, les attaques par exfiltration[1070] concernent tant la phase d'apprentissage que celle d'utilisation des SIA mais interviennent majoritairement durant la phase d'utilisation. Ces attaques sont susceptibles de porter atteinte à la confidentialité des DACP des personnes concernées par le traitement et *de facto* leur protection à la vie privée. Les attaques par exfiltration se divisent en trois catégories : les attaques par inférence d'appartenance, les attaques par inversion et les attaques d'extraction de modèle. Les attaques par inférence d'appartenance consistent pour l'attaquant « à déterminer si un point de données particulier a été utilisé pour l'apprentissage du modèle d'IA »[1071]. Ces attaques peuvent être assimilées au vol de données par rétro-ingénierie qui consiste à « reconstituer le code-source utilisé en vue de l'exploiter à des fins personnelles, voire de remonter aux données d'entrainement "mémorisées" par le modèle lesquelles peuvent présenter une certaine

---

[1065] LINC-CNIL, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *op. cit.*, p. 14.

[1066] NELSON (B.) *et al.*, "Exploiting Machine Learning to Subvert Your Spam Filter", *1st USENIX Workshop on Large Scale Exploits and Emergent Threats*, April 2008 [en ligne].

[1067] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 126.

[1068] LINC, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *op. cit.*, p. 16. Pour exemple : LIU (Y.) *et al.*, "Trojaning Attack on Neural Networks", *Department of Computer Science Technical Reports*, 2017 Paper 1781 [en ligne].

[1069] Voir pour exemple : GU (T.), DOLAN-GAVITT (B.) and GARG (S.), "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain", IEE 2019, [en ligne].

[1070] Voir à ce sujet : RIGAKI (M.) and GARCIA (S.), "A Survey of Privacy Attacks in Machine Learning", April 1st 2021 [en ligne].

[1071] LINC, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *op. cit.*, p. 17.

sensibilité »[1072] telles que les DACP ou des données secret-défense. Ce type d'attaque peut avoir lieu sur différents types de données, dont les images[1073]. Les attaques par inversion ciblent les données d'apprentissage en soumettant de nouvelles données d'entrée au SIA et en observant les résultats en sortie[1074]. Ces attaques peuvent également porter sur des données images et permettre de reconstituer les images d'entrainement[1075].

412. Cette analyse met en lumière l'importante diversité des attaques pouvant affecter spécifiquement les SIA et, par conséquent, les algorithmes « augmentés » des drones aériens de sécurité publique. Toutefois, aux yeux des chercheurs en informatique, ces attaques demeurent relativement théoriques et nécessitent un certain niveau d'expertise[1076]. Néanmoins, le recours croissant aux SIA et l'augmentation des compétences dans ce domaine requièrent l'adoption de mesures techniques permettant d'anticiper et de pallier ces nouveaux types d'attaques. Le recours à des technologies « augmentées » à des fins de sécurité publique engendrent ainsi de nombreuses limitations aux droits et libertés des personnes circulant sur la voie publique dont principalement le droit à la vie privée. Si ces limitations étaient déjà présentes au travers des systèmes de vidéoprotection, leur association à des algorithmes d'analyse d'images pourrait porter atteinte à certaines libertés, telles que la liberté individuelle, ou à certains principes, telles que la non-discrimination ou encore les droits de la défense. Mais au-delà des limitations portées aux droits et libertés, les drones aériens « augmentés » de sécurité publique tendent également à modifier les fondements de l'État de droit qui reposent principalement sur le caractère régalien des activités de police et sur le respect des principes inhérents à la procédure pénale.

[1072] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 126.

[1073] HAYES (J.) et al., "LOGAN: Membership Inference Attacks Against Generative Models", *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2019, Issue 1. August 21st 2018 [en ligne].

[1074] Ce type d'attaque suppose par conséquent de disposer de privilèges élevés (contrôle administrateur) et d'avoir une bonne connaissance du SIA ciblé.

[1075] FREDRIKSON (M.), JHA (S.) and RISTENPART (T.), "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures", *ACM CCS'15,* October 12–16, 2015 [en ligne] ; ZHANG (Y.) *et al.*, "The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks", April 18th 2020 [en ligne].

[1076] LINC, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *op. cit.*, p. 21.

CHAPITRE 2 LES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE, VECTEURS D'UNE REDÉFINITION DE L'ÉTAT DE DROIT

413. D'une manière générale, le recours aux technologies de surveillance de la voie publique renforce le débat quant à l'implication du secteur privé au sein des activités régaliennes de sécurité publique et de son incidence sur la définition du périmètre de la force publique. La coproduction de sécurité entre acteurs publics et privés, largement plébiscitée par les Gouvernements qui se sont succédés, a contraint les juges tant administratifs que constitutionnels à reconsidérer ce qui relevait des activités de service public délégables de celles qui ne l'étaient pas (**Section 1**).

414. Aussi, le recours croissant aux technologies de surveillance par les forces de l'ordre tend à installer durablement des règles d'exception au motif d'assurer la sauvegarde de l'ordre public et d'aider à la recherche des auteurs d'infractions. Les drones aériens « augmentés » de sécurité publique n'ont pas uniquement vocation à prévenir les troubles à l'ordre public par l'observation des images mais se destinent à la recherche d'auteurs d'infractions et par conséquent à la collecte de preuves pouvant servir lors du procès pénal. Néanmoins, le traitement qu'assurent les systèmes d'aide à la prise de décisions (SAAD) pourrait avoir une influence sur la preuve pénale. Il convient donc de s'interroger sur la nécessité de faire usage de certains types de SAAD par les forces de l'ordre. Il s'agira ensuite d'effectuer une évaluation générale de l'incidence sur l'État de droit du recours croissant aux nouvelles technologies de surveillance au sein de l'espace public (**Section 2**).

Section 1 Les algorithmes « augmentés » à des fins de sécurité publique : délégation d'activités ou de pouvoirs de police ?

415. Depuis l'émergence des nouvelles technologies, le secteur privé s'immisce de manière toujours plus prégnante au sein des activités de sécurité publique généralement attribuées aux forces de l'ordre[1077]. La politique de sécurité actuelle fait régulièrement état d'une volonté d'impliquer davantage le secteur privé dans les activités de sécurité comme en témoigne le discours d'Ouverture de Gérard Collomb aux 5ème assises de la sécurité privée le 5 février 2018[1078]. Lors de la publication de la LOPS en 1995, les pouvoirs publics accordaient déjà une grande importance à cette

[1077] En ce sens, le CSI dédit son Livre VI aux activités privées de sécurité (art. L. 611-1 à L. 648-1).

[1078] Discours de Gérard COLLOMB, ministre d'État, ministre de l'Intérieur, Ouverture des 5ème assises de la sécurité privée, 5 février 2018 [en ligne].

coopération, assurant que la sécurité privée concourait à la sécurité générale de l'État[1079]. Aux dires du professeur Olivier Gohin, « la sécurité privée n'aurait pas vocation à se substituer à la force publique mais à l'accompagner dans le respect des prérogatives qui sont les siennes »[1080]. Depuis une dizaine d'années, il est ainsi largement admis que la sécurité s'inscrit sous la forme d'une collaboration entre les acteurs publics et les acteurs privés[1081]. La publication du Livre blanc de la sécurité intérieure en fait d'ailleurs mention dès son introduction énonçant que « la sécurité privée (entreprises, services internes de sécurité) est déjà et sera encore plus à l'avenir un partenaire du *continuum* [de sécurité] »[1082] tout en insistant sur le besoin de mettre en place des garanties de contrôle. En outre, la loi « sécurité globale » entendait également concrétiser les intentions de renforcement de cette collaboration entre acteurs publics et acteurs privés au sein de la sécurité publique[1083]. Ces dispositions ont cependant été rejetées par le Conseil constitutionnel, qui les avaient déclarées comme inconstitutionnelles au motif qu'elles contrevenaient à l'article 12 de la DDHC[1084].

416. Ce phénomène d'association des acteurs privés (parfois décentralisés ou même transnationaux) aux missions de sécurité retient, toutefois, l'attention d'une partie de la doctrine qui perçoit une potentielle remise en question de la souveraineté[1085] ainsi que du monopole de la violence légitime[1086] couramment attribué à l'État[1087]. En d'autres termes, elle l'interprète comme

---

[1079] LATOUR (X.), « Des activités privées de sécurité des agences de recherche privées dans le code de la sécurité intérieure », *in* MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, *op. cit.*, p. 196.

[1080] GOHIN (O.), « La Constitution, ultime obstacle à la privatisation de la sécurité ? », *op. cit.*

[1081] Voir notamment : BAUER (A.) et VENTRE (A-M.), *Les polices en France*, Paris, PUF, « Que sais-je ? », 2010, 128 p., p. 99 ; LATOUR (X.), « L'article 12 de la Décoration des droits de l'homme et du citoyen et le Conseil constitutionnel » *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 31-39 ; LATOUR (X.) et MOREAU (P.), « Le Conseil national des activités privées de sécurité et la moralisation de la sécurité privée », *JCP A* n° 15, 11 avril 2011, 2146 ; LATOUR (X.), « Sécurité publique et sécurité privée, de l'ignorance à la coproduction », *Cahiers de la sécurité* n° 19, 2012, p. 11.

[1082] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*, p. 6.

[1083] Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.*, art. 29.

[1084] C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.*, cons. 59.

[1085] BEAUD (O.), *La puissance de l'État*, Paris, PUF, Léviathan, 1994, 512 p., p. 102.

[1086] WEBER (M.), *Le savant et le politique*, Paris, La Découverte, 2003, 210 p., p. 118 ; ELIAS (N.), *La Dynamique de l'occident*, Paris, Édition Pocket, Évolution, 2003, 320 p.

[1087] De manière non exhaustive : COSSALTIER (P.), « L'intervention du secteur privé dans les activités de sécurité publique : à la recherche d'une limite » *in* PAULIAT (H.), *La sécurité intérieure en Europe*, PULIM, 2010, pp. 45-75 ; LATOUR (X.), « La place du secteur privé dans la politique moderne de sécurité », *AJDA*, 2010, p. 657 ; LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *JCP A* n° 15, 15 avril 2012, 2117 ; GOHIN (O.), « La Constitution, ultime obstacle à la privatisation de la sécurité ? », *Les Cahiers de la sécurité*, mars 2012, p. 18 ; MOREL (B.), « L'attribution d'activités de police à des personnes privées », *RDP*, 1er janvier 2020, p. 77.

une attribution de pouvoirs de police administrative à des entités privées bien que la police soit généralement perçue comme une « fonction de protection de l'ordre statutaire primaire libérale »[1088] inhérente à l'existence même de l'État. Les activités de sécurité, propres au pouvoir de police, seraient ainsi en partie déléguées à des personnes privées. À l'inverse, certains auteurs soutiennent que rien ne s'oppose à la délégation de l'exécution de missions de police à des personnes privées soumises au contrôle de l'État délégant[1089].

417. En vue d'appréhender le sens de ces interprétations, il convient, dès lors, de définir les notions de « pouvoir de police » et de « délégation ». Le « pouvoir de police » peut être défini de manière générale comme « la fonction disciplinaire de l'institution politique globale […] consistant à mettre en œuvre les exigences de l'ordre public au sein de cette institution politique globale »[1090]. La notion de « délégation » désigne, au sens général du terme, le fait par une personne de transmettre une mission ou une fonction à une autre personne. Pour les publicistes, « elle est assimilée à un acte unilatéral en vertu duquel une autorité publique […] transfère l'exercice d'une partie de sa compétence »[1091]. En d'autres termes, lors d'une délégation, le délégant attribue, sous son contrôle, l'exercice d'une mission au délégataire. La question de savoir s'il était possible pour les autorités publiques de déléguer leur pouvoir de police à des personnes privées qui en exerceraient les missions a fait l'objet d'un long parcours jurisprudentiel[1092].

418. Aujourd'hui, la volonté exprimée par l'État de renforcer la coopération des secteurs publics et privés au maintien de la sécurité publique, notamment par le recours à des algorithmes « augmentés » interroge l'existence même du caractère régalien propre aux missions de sécurité. Les questions entourant l'implication croissante du secteur privé au sein des activités de sécurité

1088 PICARD (E.), *La notion de police administrative*, *op. cit.*, p. 796.

1089 PAUVERT (B.), « Le pouvoir de police ne se délègue-t-il vraiment pas ? », *in* DESCHAUX-DUTARD (D.) et VIDELIN (J-C.) (dir.), *Annuaire du droit de la sécurité et de la défense 2020*, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, 2020, 252 p.

1090 PICARD (E.), « Police », *in* ALLAND (D.) et RIALS (S.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, p. 1163.

1091 FONTBAUSTIER (L.), « Délégation », *in* ALLAND (D.) et RIALS (S.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, p. 263.

1092 De manière non exhaustive : CE, ass., 17 juin 1932, n° 12045, *Ville de Castelnaudary*, Rec. CE 1932 p. 595 [en ligne] ; CE, sect. 23 mai 1958, n°s 35737, 31976, 32078, *Consorts Amoudruz*, Rec. p. 301 ; C. cass., ch. crim., 27 mai 1972, n° 71-91607 [en ligne] ; CE, 29 juillet 1983, n° 15116, *Baffroy-Lafitte* ; CE, 6ème et 2ème ss-sect. réunies 30 septembre 1983, n° 26611, *Fédération départementale associations agréées de pêchée l'Ain*, Rec. CE 1983, p. 392 [en ligne] ; CE, 7ème et 10ème ss-sect. réunies, 1er avril 1994, n° 144152-144241, *Commune de Menton*, Rec. CE 1994, p. 175 [en ligne] ; CE, 29 décembre 1997, n° 170606, *Commune d'Ostricourt*, Rec. CE 1997, p. 969 [en ligne] ; CE, 19 décembre 2007, n° 260327, *Sté Sogeparc* [en ligne].

méritent un examen plus approfondi de la délégation de fonctions étatiques (§1). À cette question s'ajoutent les préoccupations liées à la « dépendance » des acteurs chargés de préserver l'ordre public aux produits et services issus d'entreprises privées. En outre, certaines de ces entreprises sont étrangères ce qui renforce la fragilisation des mécanismes de souveraineté nécessaires aux activités liées à l'exercice de la force publique (§2).

§1. Le principe d'interdiction de déléguer des pouvoirs de police : analyse jurisprudentielle et doctrinale

419. En droit français, la doctrine comme la justice ont régulièrement réaffirmé la formule énonçant que « les pouvoirs de police ne se délèguent pas, ni ne s'exercent par voie contractuelle »[1093]. Elle fut même érigée au rang de principe bénéficiant d'une double protection juridique : du Conseil d'État, d'une part, et du Conseil constitutionnel, d'autre part (A). Pourtant, ce principe semble nuancé en pratique par ces mêmes juridictions. Plusieurs raisons ont été avancées pour expliquer l'évolution de l'interdiction de délégation[1094] telle que la crise budgétaire de l'État (incitant des modifications dans la répartition des moyens), le sentiment d'insécurité exprimé par la population, mais aussi une offre de sécurité venant du secteur privé (principalement dans le domaine technologique).

420. La question portant sur la coproduction de la sécurité par l'État et les acteurs privés nécessite une étude des contours de la notion de délégation afin de déterminer ce qui peut faire l'objet d'une délégation. Le constat d'un effritement du principe par une évolution législative emprunte d'une « volonté constante d'innover en externalisant »[1095] mérite une analyse approfondie de la jurisprudence récente, particulièrement lorsqu'elle porte sur le recours à des nouvelles

---

[1093] PETIT (J.), « Nouvelles d'une antinomie : contrat et police », p. 345 *in* PETIT (J.), *Les collectivités locales. Mélanges en l'honneur de Jacques Moreau*, Paris, Economica, 2003, 491 p. ; ECKERT (G.), « Police et contrat », p. 167 *in* VAUTROT-SCHWARTZ (Ch.) (dir.), *La police administrative*, PUF, 2014, 320 p. ; PRÉTOT (X.) et ZACHARIE (C.), *La police administrative*, Paris, LGDJ, coll. Systèmes, 2018, 162 p., p. 66 ; PLESSIX (B.), *Droit administratif général*, Paris, LexisNexis, 3ème édition, 2020, 1742 p., n° 205 et suiv. et n° 621 et suiv. ; MOREAU (J.), « De l'interdiction faite à l'autorité de police d'utiliser une technique d'ordre contractuel », *AJDA*, 1965, p. 3 ; LEMAIRE (E.), « Actualité du principe de prohibition de la privatisation de la police », *AJDA*, 2009, p. 767 ; MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

[1094] LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *op. cit.*

[1095] LATOUR (X.), « L'article 12 de la Déclaration des droits de l'homme et du citoyen et le Conseil constitutionnel », pp. 31-39, spéc. p. 32 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*

technologies (B).

A. L'affirmation du principe d'interdiction de la délégation

421. La position adoptée par le juge administratif - Le Conseil d'État fut le premier a être saisi de la question concernant la délégation au privé en matière de sécurité dans un arrêt du 17 juin 1932, *Ville de Castelnaudary*. Dans le cadre de sa décision, le Conseil d'État a estimé que « le service de la police rurale, par sa nature, ne saurait être confié qu'à des agents placés sous l'autorité directe de l'Administration »[1096]. Il a ainsi posé pour la première fois le principe d'interdiction de délégation du pouvoir de police se fondant sur la théorie de l'indisponibilité des compétences[1097] et de la théorie des droits acquis[1098]. Il a réaffirmé ce principe à de nombreuses reprises, notamment dans sa décision *Association les amis de la Terre* du 8 mars 1985[1099].

422. Deux décisions de principe témoignent également de la volonté d'interdire de manière stricte toute délégation. Dans le premier arrêt, *Commune de Menton*, le Conseil d'État a annulé les conventions établies entre la commune et une société privée à des fins de gestion du stationnement payant[1100]. Le Conseil d'État a affirmé que « le service de la police et du stationnement, par sa nature, ne saurait être confié qu'à des agents placés sous l'autorité directe du maire »[1101]. Le juge administratif a ainsi consacré l'interdiction d'avoir recours au procédé contractuel en matière de police. Le deuxième arrêt, *Commune d'Ostricourt*, confirme l'interdiction de déléguer des pouvoirs de police à une autre personne (publique ou privée) et d'établir certains contrats en matière de police[1102]. À l'origine, le juge administratif s'était ainsi opposé à toute forme de délégation

---

1096 CE, ass., 17 juin 1932, *Ville de Castelnaudary*, *op. cit.*

1097 Il s'agit du fait que des compétences qui ont été attribuées à une autorité ne puissent faire l'objet d'une subdélégation par cette dernière. Sur ce sujet voir notamment : AZOUAOU (P.), *L'indisponibilité des compétences en droit public interne*, Mare & Martin, Thèse, 2016, pp. 243-252.

1098 MOREAU (J.), « De l'interdiction faite à l'autorité de police d'utiliser une technique d'ordre contractuel », *op. cit. ;* PERRIER (M.), *Le recours au contrat en matière de police administrative*, Thèse, Lyon III, 2011, pp. 328-355 cité par MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

1099 CE, 8 mars 1985, n° 24557, *Association les amis de la Terre* [en ligne].

1100 CE, 1er avril 1994, *Commune de Menton*, *op. cit.*

1101 *Idem*.

1102 Le Conseil d'État avait ainsi censuré le contrat établi entre la commune d'Ostricourt et une société privée de surveillance et de gardiennage à des fins de surveillance de la ville au motif « qu'un tel contrat, qui ne se limitait pas à confier à la société [privée] des tâches de surveillance et de gardiennage […] avait pour effet de lui faire assurer une mission de surveillance des voies publiques de l'ensemble de la commune » (CE, 29 décembre 1997, *Commune d'Ostricourt*, *op. cit.*).

contractuelle en matière de police et ce principe semblait être unanimement adopté par la doctrine[1103]. Dès lors, l'interdiction de déléguer des pouvoirs de police à des personnes privées serait un principe unanimement reconnu et fondamental du droit de la police administrative[1104]. Le juge administratif fonde ses décisions sur l'opposition entre la nature du contrat et celle de la police.

423. Le principe d'interdiction posé par le juge administratif porte autant sur la délégation contractuelle que sur la délégation unilatérale[1105]. En d'autres termes, il s'applique tant au « transfert d'une activité normative à une personne privée » qu'à « l'habilitation de celle-ci à exercer des activités matérielles de police »[1106]. L'interdiction pour une autorité de recourir au procédé contractuel afin de déléguer ses pouvoirs en matière de police administrative est « constitutive d'un moyen d'ordre public »[1107] et fut mainte fois réitérée dans la jurisprudence administrative[1108]. En outre, dans un arrêt du 8 juillet 2005, le Conseil d'État a conclu au caractère imprescriptible du pouvoir de police indiquant que celui-ci ne s'éteint, pas même par son non-usage prolongé[1109]. Néanmoins, une difficulté subsiste concernant la détermination de ce qui relève du pouvoir de police, qui ne peut être délégué dans le cadre d'un contrat, et ce qui constitue une activité matérielle de police, qui peut faire l'objet d'une délégation.

[1103] En ce sens, le professeur Maurice Hauriou écrivait que « d'une façon générale, on ne concevrait pas, dans notre droit, l'utilisation de corps de police particuliers et privés » (HAURIOU (M.), note sous CE, 24 décembre 1909, *Commune de Bassée* : S. 1910, III, p. 49). Plus tard, le professeur Jacques Petit a affirmé que : « cette […] prohibition est largement entendue. Elle couvre les activités juridiques, soit le transfert d'un pouvoir de décision par son titulaire normal à une autre personne privée ou publique. L'autorité de police ne saurait davantage se décharger sur un tiers des activités matérielles qui lui incombent » (PETIT (J.), « Nouvelles d'une antinomie : contrat et police », p. 345 *in* PETIT (J.), *Les collectivités locales. Mélanges en l'honneur de Jacques Moreau*, *op. cit.*). Le principe était également affirmé par le professeur Jacques Moreau (voir notamment : MOREAU (J.), « De l'interdiction faite à l'autorité de police d'utiliser une technique d'ordre contractuel », *op. cit.*).

[1104] MOREAU (L.), « La contractualisation de l'exercice de la police administrative », pp. 171-190, *in* CLAMOUR (G.) et UBAUD-BERGERON (M.) (dir.), *Contrats publics. Mélanges en l'honneur du Professeur Guibal*, Montpellier, PUM, 2006, 1588 p.

[1105] Voir en ce sens : CE, 7ème et 10ème ss-sect. réunies, 10 décembre 1962, n° 55284, *Association de pêche et de pisciculture d'Orléans*, Rec, p. 675 ; CE, 6ème et 2ème ss-sect. réunies, 30 septembre 1983, n° 31875, 31910 31945 31948 32034 [en ligne].

[1106] TA Versailles, 17 janvier 1986, *Commissaire de la République du département de Seine-et-Marne*, Rec, p. 303.

[1107] MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

[1108] Voir en ce sens : TA Paris, 27 février 1963, *Société des établissements Lick et brevets Paramount*, Rec, p. 689 ; TA Versailles, 19 octobre 1984, *Blanchard et Monbrun*, Rec, p. 463 ; CAA Bordeaux, 2ème ch., 28 avril 1997, n° 96BX01843, *Commune d'Alès*, Rec T., p. 972 [en ligne] ; CAA Marseille, 3ème ch., 26 juin 2003, n° 99MA01920, *Compagnie générale de stationnement* : *RDA* 2003, p. 21 [en ligne] ; CE, 7ème et 2ème ss-sect. réunies, 11 mai 2009, n° 296919, *Ville de Toulouse* : *AJDA* 2010, p. 634 [en ligne].

[1109] CE, ass., 8 juillet 2005, n° 247976, *Sté Alusuisse-Lonza-France*, Rec., p. 311 [en ligne].

424. La position adoptée par le juge constitutionnel - Le Conseil constitutionnel intervient également sur les questions relatives à la délégation de pouvoirs de police. Il a émis ses premières décisions en la matière dans les années 1980 où il a fait mention de l'existence de « services publics constitutionnels »[1110] qui ne peuvent faire l'objet d'une délégation[1111] et auxquels appartiennent les pouvoirs de police[1112]. Lors de sa décision du 25 février 1992[1113], il a affirmé sa volonté de défendre le principe d'interdiction de la délégation de missions de police administrative à des agents privés. Depuis sa décision du 29 août 2002[1114], il opère une distinction entre les pouvoirs régaliens de police et les missions matérielles. À cette occasion, le Conseil constitutionnel a effectué son contrôle des dispositions octroyant des fonctions de service public pénitentiaire à des personnes privées en vérifiant qu'elles n'entraient pas dans le cadre des « tâches inhérentes à l'exercice par l'État de ses missions de souveraineté »[1115]. Ainsi, il a déclaré comme étant inconstitutionnelles toutes formes de délégation de prérogatives de puissance publique lorsque celles-ci étaient indissociables « des fonctions de souveraineté »[1116].

425. Par la suite, le juge constitutionnel avait adopté une autre approche, considérant la délégation de pouvoirs de police comme remettant en cause la portée de l'article 12 de la DDHC

[1110] DE BELLESCIZE (R.), *Les services publics constitutionnels*, Paris, LGDJ, coll. Bibliothèque de droit public, Thèse, 2005, 486 p.

[1111] Voir notamment la décision du Conseil constitutionnel du 26 juin 1986 où il souligne « qu'en ne prenant pas le soin de déterminer lui-même la nature de l'autorité administrative devant approuver les opérations de transfert visées au paragraphe II de l'article 7, le législateur a opéré une subdélégation non permise par la Constitution » (C. const., Décision n° 86-207 DC, 26 juin 1986, *Loi autorisant le Gouvernement à prendre diverses mesures d'ordre économique et social*, cons. 77, *JORF*, 27 juin 1986 [en ligne].

[1112] FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, Paris, Dalloz, 20ème édition, 2022, 1128 p., pp. 243-258.

[1113] C. const., Décision n° 92-307 DC, 25 février 1992, *Loi portant modification de l'ordonnance n° 45-2658 du 2 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France*, *JORF*, 12 mars 1992, cons. 32 : le juge constitutionnel affirme à cette occasion que les dispositions de l'ordonnance « ne saurai[en]t ainsi s'entendre comme conférant au transporteur un pouvoir de police aux lieu et place de la puissance publique ».

[1114] C. const., Décision n° 2002-461 DC, 29 août 2002, *Loi d'orientation et de programmation pour la justice*, *JORF* du 10 septembre 2002, cons. 8 et 9 [en ligne] : S'agissant du placement sous surveillance électronique, le juge constitutionnel avait estimé que la disposition autorisant que des « fonctions autres que celles de direction, de greffe et de surveillance [puissent être] confiées à des personne de droit public ou de droit privé habilitées, dans des conditions définies par un décret en Conseil d'État » n'était pas contraire à la Constitution.

[1115] *Idem*, cons. 8 : « s'agissant des fonctions mentionnées […] dont sont expressément exclues les tâches inhérentes à l'exercice par l'État de ses missions de souveraineté, leur délégation fera l'objet d'une habilitation dans les conditions définies par décret en Conseil d'État ».

[1116] *Idem*. Voir aussi : C. const., Décision n° 2003-473 DC, 26 juin 2003, *Loi habilitant le Gouvernement à simplifier le droit*, cons. 19, *JORF*, 3 juillet 2003 [en ligne] ; C. const., Décision n°2003-484 DC, 20 novembre 2003, *Loi relative à la maitrise de l'immigration, au séjour des étrangers en France et à la nationalité*, *op. cit.*, cons. 87, 88, 89, 90 : dans cette décision, le juge constitutionnel a reconnu comme contraire à la Constitution la délégation à des personnes privées des missions de surveillance d'étrangers en situation irrégulière.

qui énonce que « la garantie des droits de l'homme et du citoyen nécessite la force publique : cette force est donc instituée pour l'avantage de tous et non pour l'utilité particulière de ceux auxquels elle est confiée ». Depuis sa décision du 10 mars 2011 portant sur la LOPPSI[1117], le juge constitutionnel consacre son rattachement à l'article 12 de la DDHC en matière d'interdiction de délégation de pouvoirs de police au privé. À cette occasion, il avait censuré plusieurs dispositions de cette loi qui prévoyaient notamment d'autoriser la délégation du visionnage des voies publiques à un opérateur privé[1118]. Il avait déclaré cette disposition comme contraire à la Constitution en invoquant l'article 12 de la DDHC, estimant qu'elle permettait d' « investir des personnes privées de missions de surveillance générale de la voie publique [ce qui] rend ainsi possible la délégation à une personne privée des compétences de police administrative générale inhérentes à l'exercice de la "force publique" nécessaire à la garantie des droits »[1119]. Cette décision a symbolisé un tournant dans la jurisprudence constitutionnelle[1120] tant par la continuité du fondement[1121] que par son rattachement à un texte « dépourvu d'ambiguïté »[1122]. En outre, elle n'entre pas en contradiction avec celles précédemment émises. Depuis lors, la jurisprudence constitutionnelle fonde exclusivement sa protection des missions relevant de la force publique sur l'article 12 de la DDHC.

426. Le juge administratif et le juge constitutionnel œuvrent ainsi de concert en faveur d'une interdiction, par principe, de toute forme de délégation des pouvoirs de police. Néanmoins, il apparait incontestable que le principe admet depuis plusieurs années certaines interprétations voire exceptions afin de satisfaire les pouvoirs publics dans leur quête de co-productivité de la sécurité, amenant un dépassement de l'interdiction de la délégation.

1117 C. const., Décision n°2011-625 DC, 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011*, *JORF* 15 mars 2011, p. 4630 [en ligne].

1118 LOPPSI, art. 18.

1119 C. const., Décision n°2011-625 DC, 10 mars 2011, *op. cit.*, cons. 19.

1120 MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

1121 Le fondement sera repris dans plusieurs décisions : C. const., Décision n° 2017-637 QPC, 16 juin 2017, *Association nationale des supporters*, *JORF* n° 0141, 17 juin 2017, cons. 4 [en ligne] ; C. const., Décision n° 2019-810 QPC, 25 octobre 2019, *Société Air France*, *JORF* n° 0250, 26 octobre 2019, cons. 11 et 12 [en ligne] ; C. const., Décision n° 2019-781 DC, 16 mai 2019, *Loi relative à la croissance et la transformation des entreprises*, *JORF* n° 0119, 23 mai 2019 [en ligne].

1122 LATOUR (X.), « L'article 12 de la Déclaration des droits de l'homme et du citoyen et le Conseil constitutionnel », pp. 31-39, spéc. p. 34 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.* Voir aussi : GOHIN (O.), « La constitution, ultime obstacle à la privatisation de la sécurité ? », *op. cit.*, pp. 19-26.

B. L’assouplissement du principe d’interdiction de la délégation

427. Le principe interdisant à des personnes publiques de déléguer des missions de police inhérentes à l’exercice de la force publique à des personnes privées, bien que régulièrement confirmé par la jurisprudence administrative, fait l'objet d'une atténuation par ce dernier. Ce principe, qui se voulait immuable, est souvent remis en question par l’introduction du secteur privé dans le champ de la sécurité[1123]. À l’appui de ce constat, l’édification du Code de la sécurité intérieure aura permis d’insérer le secteur privé dans les activités de sécurité, au travers du livre IV qui s’intitule « Activités privées de sécurité »[1124], admettant de ce fait que les activités de sécurité puissent être exercées tant par des acteurs publics que privés[1125]. L’introduction du secteur privé dans les activités de sécurité a suivi un long processus jurisprudentiel avant d’être finalement reconnue par une succession de lois dès les années 1980[1126]. Le monopole public des fonctions de police administrative a parfois fait l’objet de dérogations au principe, au point que certains auteurs se prêtent à dire qu’il serait erroné « de faire de la police un attribut régalien qui serait le monopole de l’État »[1127] (1). Dès lors, la décision du Conseil constitutionnel de 2011 pouvait surprendre[1128] au regard de sa décision précédente concernant la loi du 23 janvier 2006[1129] autorisant notamment à des personnes privées d’installer des dispositifs de surveillance de la voie publique à des fins de

---

[1123] Voir notamment en ce sens : MOREAU (J.), « De l’interdiction faite à l’autorité de police d’utiliser une technique d’ordre contractuel », *op. cit.* ; LEMAIRE (E.), « Actualité du principe de prohibition de la privatisation de la police », *op. cit.* ; LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *op. cit.* ; PRÉTOT (X.), « Le pouvoir de police ne se concède pas : un principe inhérent à l’identité constitutionnelle de la France à la portée toute relative… », *JCP A* n° 48, 6 décembre 2021, 2373, ; LATOUR (X.), « L’article 12 de la Décoration des droits de l’homme et du citoyen et le Conseil constitutionnel », pp. 31-39, spéc. p. 36 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*

[1124] CSI, art. L. 611-1 et s.

[1125] DESPREZ (F.) et VIENNOT (C.), « Les incertitudes du Code de la sécurité intérieure à propos des activités privées de sécurité », p. 105 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d’un nouvel ordre ou semeur de désordre ?*, *op. cit.*

[1126] Voir notamment : Loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de surveillance, de gardiennage et de transports de fonds, *JORF* du 13 juillet 1983 [en ligne] ; Loi n° 95-73 du 21 janvier 1995 d’orientation et de programmation relative à la sécurité, *op. cit.* ; Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *JORF* n°266 du 16 novembre 2001 [en ligne] ; Loi n° 2002-1094 du 29 août 2002 d’orientation et de programmation pour la sécurité intérieure, *op. cit.* ; Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, *op. cit.*

[1127] MOREL (B.), « L’attribution d’activités de police à des personnes privées », *op. cit. ;* voir aussi RENAUDIE (O.), « Police et service public », *in* VAUTROT-SCHWARZ (C.) (dir.), *La police administrative*, *op. cit.*, pp. 39-53 ; PAUVERT (B.), « Le pouvoir de police ne se délègue-t-il vraiment pas ? », *op. cit.*

[1128] DARSONVILLE (A.), « Décision n° 2011-625 DC du 10 mars 2011 : une censure sévère de la LOPPSI 2 ? », *Constitutions : Revue de droit constitutionnel appliqué* n°2, 2011, p. 223.

[1129] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, *op. cit.*

lutte contre le terrorisme, qu'il n'avait pas censuré[1130]. La jurisprudence tendrait ainsi à s'adapter aux besoins requis en matière d'ordre public en laissant une certaine marge de manœuvre au législateur afin d'octroyer de nouvelles missions à des acteurs privés (2).

1. L'atténuation relative du principe d'interdiction de la délégation

428. Le juge administratif est venu jeter le trouble sur le principe d'interdiction en considérant que l'exécution de certaines activités matérielles de police administrative constituait une mission de service public qui par conséquent pouvait être déléguée, sous réserve d'être effectuée sous le contrôle de l'autorité publique[1131]. Ce doute est ainsi renforcé par l'opacité de la distinction entre les activités de service public[1132] (qui peuvent être déléguées) et les missions matérielles de police (qui ne peuvent, en principe, être déléguées)[1133]. Or, les notions service public et de police se confondent dès leur origine[1134] dans la mesure où la police exerce des missions de service public[1135] et que la notion de police tend à évoluer au cours du temps du fait que « la conception de l'ordre public ne saurait être figée »[1136]. Cette confusion entre les deux notions n'est pas inédite puisqu'elle était déjà observée dans le cadre de deux éminents arrêts du Conseil d'État, Terrier et Thérond[1137]. La question de l'interprétation du principe d'interdiction reposerait sur la détermination de ce qui relève de la compétence de la police[1138] (pouvoir régalien) et de ce qui relève du service public (ici, les activités matérielles de police). Ainsi, le juge administratif a contribué à un phénomène de

---

1130 Le juge constitutionnel n'avait pas opéré de contrôle de ces dispositions lorsque la loi lui avait été déférée (C. const., Décision n° 2005-532 DC, 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, *JORF* du 24 janvier 2006 [en ligne]).

1131 CE, sect., 24 mai 1968, n° 69733, *Ministère de l'Intérieur c/ Sieur Chambrin*, Rec, p. 331 [en ligne].

1132 Dans l'arrêt *Narcy* (CE, 28 juin 1963, *Narcy*, Rec. 401.) le Conseil d'État définit les critères qualificatifs d'un service qui regroupent l'ensemble des activités assurées directement ou indirectement par l'Administration ayant pour finalité l'intérêt général dont le régime relève en partie du droit public. Néanmoins, la solution doit être lue au regard de l'arrêt APREI (CE, 22 février 2007, n° 264541, *APREI* [en ligne]) introduisant de nouveaux critères.

1133 MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

1134 PRÉTOT (X.), « Le pouvoir de police ne se concède pas : un principe inhérent à l'identité constitutionnelle de la France à la portée toute relative… », *op. cit.*

1135 Ainsi, le professeur René Chapus déclarait qu'« exercer la police administrative, c'est assurer un service public : celui du maintien de l'ordre public » (CHAPUS (R.), *Droit administratif général*, Tome I, LGDJ, coll. Précis Domat, 15ème édition, 2001, 1440 p., n° 901, p. 700).

1136 LEBRETON (G.), « Ordre public », pp. 569-570 *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*

1137 CE, sect., 6 février 1903, n° 07496, *Terrier*, Rec. 1903, III, p. 25 [en ligne] ; CE, sect., 4 mars 1910, n° 29373, *Thérond*, Rec, p. 193 [en ligne].

1138 Selon les termes du professeur Didier Truchet, les pouvoirs de police appartiennent à la catégorie des « contrats administratifs impossibles » (TRUCHET (D.), *Droit administratif*, Paris, PUF, 9ème édition, 2021, 564 p., p. 295).

confusion du principe en considérant « l'exécution de certaines activités matérielles de police administrative comme relevant simplement d'activités de service public pouvant faire l'objet de délégation dès lors qu'elles sont réalisées sous le contrôle de l'Administration »[1139]. Dès lors, la possibilité d'une délégation de missions de police repose sur la frontière entre activité matérielle de police et pouvoir de police déterminée par le juge. Toutefois, le fait de soumettre cette qualification à la seule appréciation du juge laisse le champ libre à l'interprétation du principe d'interdiction.

429. Néanmoins, pour certains auteurs, l'interprétation de la décision *Ville de Castelnaudary* est claire et exprime simplement la volonté du Conseil d'État de rappeler que le service de police ne pouvait être confié à des agents privés qu'à la condition d'être soumis à l'autorité directe de l'Administration. En d'autres termes, les juges ne considéraient nullement que les activités de police devaient être confiées exclusivement à des agents publics et n'interdisaient aucunement le fait d'attribuer leur exercice à des personnes privées. En définitive, la décision émettait une interdiction « de confier la charge [responsabilité et missions] du service à un acteur privé »[1140] sans encadrement par l'administration. Ainsi, selon ces auteurs, la formule énoncée peut paraître « réductrice et trompeuse »[1141] et ferait l'objet d'une erreur d'interprétation.

430. Dans son étude, Monsieur David Melloni[1142] soutient qu'il n'existerait réellement aucune activité qui ne puisse faire l'objet d'une délégation. Si l'auteur mentionne l'existence d'activités qui, par nature, ne sont pas délégables, il souligne le fait que cette position tient davantage « de l'affirmation de principe que de la réalité pratique »[1143]. Selon l'auteur, la délégation de fonctions étatiques à des personnes privées existe depuis l'ancien droit jusqu'à nos jours et toujours sous le contrôle de l'État. En d'autres termes, quel que soit le domaine ayant fait l'objet d'une délégation, l'État conserve son pouvoir décisionnel et laisse les modalités de mise en œuvre de l'activité déléguée aux personnes privées délégataires.

[1139] MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.* Voir en ce sens : CE, ass., 12 avril 1957, n° 23754, *Mimouni*, Rec. p. 261. [en ligne] et PICARD (É.), *La notion de police administrative*, *op. cit.*, p. 804 et 805.

[1140] PAUVERT (B.), « Le pouvoir de police ne se délègue-t-il vraiment pas ? », *op. cit.*

[1141] *Idem*.

[1142] MELLONI (D.), *Délégation de service public : du contrat à l'habilitation institutionnelle*, Nancy, Thèse, 2006, pp. 79-95 cité par PAUVERT (B.), « Le pouvoir de police ne se délègue-t-il vraiment pas ? », *op. cit.*

[1143] *Idem*. Voir également en ce sens : LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *op. cit.*

431. Dès lors, il est possible de déléguer des missions de police à des personnes privées sous réserve de respecter certaines modalités. En ce sens, le professeur Pierre Delvolvé rappelait que « la collectivité délégante ne cesse pas d'être compétente en déléguant son service public »[1144]. En pratique, l'expression « délégation de service public » est largement discutable dans le sens où la délégation ne concerne que la gestion d'un service public de police et que contrôle demeure entre les mains de la puissance publique. Cette gestion déléguée s'appliquerait également en matière de police administrative, sous réserve d'un encadrement stricte.

432. Le pouvoir d'interprétation du principe d'interdiction par le juge administratif peut être illustré par un arrêt du 9 novembre 2009 admettant la possible dérogation au principe dans le cadre de missions de surveillance confiées à une société privée[1145]. Si cette interprétation sera reconnue comme inconstitutionnelle en 2011, il ne peut qu'être constaté que la multiplication de nouvelles technologies accroît les occasions de déléguer des activités de police aux acteurs privés en les qualifiant de service public[1146]. En ce sens, le recours à des entreprises privées en matière de sécurité routière s'est amplifié, leur permettant notamment de faire usage de véhicules radars à des fins de verbalisation des infractions de stationnement[1147]. Les parlementaires estiment qu'il ne s'agit que d'un simple transport de l'outil de collecte des données pouvant servir à la qualification d'une infraction n'impliquant pas la constatation de celle-ci par des acteurs privés[1148]. Bien que le juge administratif s'assure de manière constante que l'autorité publique ne se soit pas dessaisie de ses prérogatives en matière de police, les faits démontrent que les missions d'exécution en matière de police sont de moins en moins considérées comme relevant de l'autorité de police[1149]. En définitive, le Conseil d'État adopte une interprétation plus modérée du principe d'interdiction que le Conseil

---

[1144] DELVOLVÉ (P.), « Les contradictions de la délégation de service public », *AJDA*, 1996, p. 677.

[1145] CAA Marseille, 6ème ch., 9 novembre 2009, n° 07MA00594, *Sté Vigitel* [en ligne].

[1146] MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.*

[1147] CE, 5ème et 6ème réunies, 8 juillet 2019, n° 419367 (Verbalisation automatisée par des véhicules conduits par des personnes privées) [en ligne] Voir : *AJDA*, 2020 p. 130 : En commentaire de cette décision, le professeur Léo Vanier constatait « l'affaissement du principe d'indélégabilité semblant, désormais, tout autant un lieu commun que son caractère ancestral ».

[1148] Rapport de la mission Parlementaire, « D'un *continuum* de sécurité vers une sécurité globale » remis par THOUROT (A.) et FAUVERGUE (J-M.), *op. cit.*, p. 108.

[1149] Voir notamment : CE, 7ème et 5ème ss-sect. réunies, 21 juin 2000, n° 212100 et 212101, *SARL Plage « Chez Joseph »* [en ligne] : « sous le contrôle de la commune et sans préjudice des pouvoirs qui appartiennent à l'autorité de police municipale » ; CE, 5ème et 4ème ss-sect. réunies, 10 octobre 2011, n° 337062, *Ministre de l'Alimentation, de l'Agriculture et de la Pêche* [en ligne] : le juge administratif admet qu'est associée « une personne privée à la mise en œuvre d'une opération décidée dans le cadre de pouvoirs de police [celle-ci doit] être exécutée sous le contrôle et la responsabilité de l'administration ».

constitutionnel en ce qu'il n'exclut pas la possibilité pour des personnes privées d'intervenir dans le cadre de missions de police administrative[1150].

433. Aussi, le cas de la vidéosurveillance s'avère particulièrement propice aux débats entre l'élargissement des exceptions émises par le législateur et la position stricte du Conseil constitutionnel en matière de délégation. Les évolutions législatives et jurisprudentielles tendent vers une approche atténuée du principe d'interdiction, qui s'expliquerait tant par les nécessités techniques tenant aux caméras de surveillance que par des aménagements budgétaires[1151]. En ce sens, la loi du 30 octobre 2017[1152] symbolise un tournant en autorisant l'intervention de personnes privées dans le domaine des activités de police administrative de la voie publique. De même, le Conseil constitutionnel reconnait que « les entreprises exerçant des activités privées de sécurité, du fait de leur autorisation d'exercice, sont associées aux missions de l'État en matière de sécurité publique »[1153].

2. L'adaptation du principe d'interdiction aux besoins de l'ordre public

434. Le juge constitutionnel s'est parfois montré plus malléable quant au principe d'interdiction laissant ainsi une marge de manœuvre au législateur en matière de délégation de prérogatives de police administrative, sans pour autant l'admettre. Face à la pression de la politique sécuritaire, le Conseil constitutionnel assouplit sa position au cas par cas en permettant aux forces publiques d'être assistées par les acteurs du secteur privé. Dans le cadre d'une question prioritaire de constitutionnalité (QPC) du 16 juin 2017[1154], le Conseil constitutionnel n'a pas soulevé, sur le

---

[1150] CE, 1ère et 6ème ss-sect. réunies, 4 avril 2012, n° 350952, *SNIASS* [en ligne] : « ni l'article 12 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 ni aucun autre principe constitutionnel n'exige […] que les missions de police administrative comportant l'exercice de prérogatives de puissance publique ne soient confiées par des personnes publiques qu'à des fonctionnaires ou des agents liés à elle par des contrats de droit public ».

[1151] En ce sens, le professeur Xavier Latour et l'avocat Pierre Moreau avancent que « le développement de la vidéosurveillance nécessite de créer des centres de supervisions des images communs à plusieurs personnes publiques ou privées afin de favoriser la continuité territoriale des espaces surveillés » et que « cette "privatisation" de la vidéosurveillance permettrait de diminuer les coûts de développement en les mutualisant avec une personne privé » (LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *op. cit.*).

[1152] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *op. cit.*

[1153] C. const., Décision n° 2015-463 QPC, 9 avril 2015, *M. Kamel B et autres*, *JORF* n°0085 du 11 avril 2015 page 6537 [en ligne].

[1154] C. const., Décision n° 2017-637 QPC, 16 juin 2017, *Association nationale des supporters*, *op. cit.*, cons. 5 : « En conférant aux organisateurs de manifestations sportives à but lucratif le pouvoir de refuser l'accès à ces manifestations, le législateur ne leur a pas délégué de telles compétences. Par conséquent, le grief tiré de la méconnaissance de l'article 12 de la Déclaration de 1789 doit être écarté ».

fondement de l'article 12 de la DDHC, la délégation d'un pouvoir de police administrative à des acteurs privés ayant pourtant un pouvoir décisionnel d'interdiction de stade. Dès lors, le juge constitutionnel semble progressivement adapter sa position aux demandes de l'exécutif en contournant les fondements qu'il a adopté en matière d'interdiction de délégation sans pour autant renier le principe.

435. Il a ainsi confirmé le fondement du principe d'interdiction sur l'article 12 de la DDHC mais a accentué son interprétation en élaborant une « grille d'analyse des missions subtile »[1155] afin de contourner l'inconstitutionnalité de dispositions soumises à son contrôle. Par une décision du 29 mars 2018, le Conseil constitutionnel a réaffirmé la nécessité d'exercer un contrôle des activités du délégataire[1156]. Dans le cadre de cette décision, les Sages ont été amenés à traiter de la constitutionnalité des dispositions de la loi du 30 octobre 2017[1157] et plus particulièrement celles relatives à la délégation des compétences de contrôle et de police à des agents privés de sécurité. Le juge constitutionnel a conclu qu'il appartient aux autorités publiques de prendre les dispositions afin de s'assurer que soit garantie de manière continue l'effectivité du contrôle exercé sur les personnes privées délégataires par les officiers de police judiciaire. Dès lors, le Conseil constitutionnel autorise la délégation de l'exercice de missions inhérentes au pouvoir de police à des personnes privées à la condition que cet exercice s'effectue sous le contrôle direct de la personne publique.

436. Dans une décision du 15 octobre 2021, le Conseil constitutionnel a identifié pour la première fois un « principe inhérent à l'identité constitutionnelle de la France »[1158] qui s'imposerait même au droit de l'Union européenne. À cette occasion, le juge constitutionnel a eu à se prononcer sur des dispositions du code de l'entrée et du séjour des étrangers et du droit d'asile afin de

---

[1155] LATOUR (X.), « L'article 12 de la Déclaration des droits de l'homme et du citoyen et le Conseil constitutionnel », pp. 31-39, spéc. p. 37 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*

[1156] C. const., Décision n° 2017-695 QPC, 29 mars 2018, *M. Rouchdi B*, *Mesures administratives de lutte contre le terrorisme*, *JORF* n°0075 du 30 mars 2018, cons. 27 [en ligne] : « Il résulte des dispositions contestées que ces personnes ne peuvent toutefois qu'assister les agents de police judiciaire et sont placées "sous l'autorité d'un officier de police judiciaire". Il appartient aux autorités publiques de prendre les dispositions afin de s'assurer que soit continûment garantie l'effectivité du contrôle exercé sur ces personnes par les officiers de police judiciaire. Sous cette réserve, ces dispositions ne méconnaissent pas les exigences découlant de l'article 12 de la Déclaration de 1789 ».

[1157] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *op. cit.* : Texte introduisant des dispositions permettant d'instituer des « périmètres de protection » (CSI, art L. 226-1).

[1158] C. const., Décision n° 2021-940 QPC, 15 octobre 2021, *Société Air France*, *JORF* n°0242 du 16 octobre 2021, cons. 9 [en ligne] voir commentaires : PRÉTOT (X.), « Le pouvoir de police ne se concède pas : un principe inhérent à l'identité constitutionnelle de la France à la portée toute relative… », *op. cit.* ; MORALES (M.), « L'interdiction de déléguer à une personne privée une compétence de police administrative : une règle inhérente à l'identité constitutionnelle de la France », *DA* n°2, février 2022, comm. 10.

déterminer si celles-ci avaient pour effet de déléguer à des personnes privées des compétences de police administrative. Lors de l'examen des dispositions, le juge constitutionnel a confirmé sa position concernant « l'interdiction de déléguer à des personnes privées des compétences de police administrative générale inhérentes à l'exercice de la « force publique » »[1159] en s'appuyant sur l'article 12 de la DDHC. Cette décision s'inscrit ainsi dans la continuité des précédentes décisions du Conseil constitutionnel et du juge administratif de maintenir les contours de la force publique.

437. Au constat de l'assouplissement des décisions jurisprudentielles, les professeurs Léo Vanier et Xavier Latour reconnaissent l'existence d'une dimension économique imposante permettant un recours accru au secteur privé dans une nouvelle approche de la police administrative. Aussi, l'omniprésence de la technologie au sein des activités de sécurité publique soulève également des interrogations quant à la place occupée par les entreprises privées, dont l'intervention sera indéniablement facilitée[1160]. Les possibilités de délégation à des acteurs privés par l'intermédiaire des nouvelles technologies devraient ainsi s'amplifier dès lors qu'un lien aura été établi avec la force publique. Aujourd'hui, la question se pose de savoir si le principe d'interdiction conserverait son sens quant à l'usage de SAAD permettant une analyse d'images issues de caméras en vue de contribuer au processus décisionnel dans le cadre de missions de police.

438. L'interdiction absolue de délégation de pouvoirs de police au secteur privé repose en partie sur le fondement de l'indisponibilité des compétences qui, pour rappel, consiste pour l'autorité publique à ne pouvoir confier celles-ci à une autre personne. Néanmoins, le juge administratif admet la possibilité pour les autorités publiques de déléguer des missions de sécurité publique sous réserve de les exercer sous le contrôle de l'Administration. À cette fin, le recours à des acteurs privés délégataires sous le contrôle de l'Administration bénéficie d'une double garantie par un maintien sous l'autorité directe, d'une part, et par la présence d'agents représentants de la force publique, d'autre part[1161]. En d'autres termes, le fait de déléguer des missions de sécurité

[1159] *Idem*, cons. 15.

[1160] LATOUR (X.), « L'article 12 de la Décoration des droits de l'homme et du citoyen et le Conseil constitutionnel », pp. 31-39, spéc. p. 38 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*

[1161] PICARD (É.), *La notion de police administrative*, *op. cit.*, pp. 15 et 16.

publique ne confère pas d'autorité décisionnelle à des entités privés ce qui empêche toute subdélégation de leurs missions qui ôterait le contrôle direct exercé par l'Administration[1162].

439. L'obligation d'exercer un contrôle de la délégation de missions de police à des personnes privées écarte ainsi toute possibilité de subdéléguer cette tâche car elle ôterait toute forme de contrôle direct par l'autorité publique. Néanmoins, le recours à un SAAD en matière de police, tel que pour les drones aériens « augmentés » de sécurité publique, interroge quant à la possibilité qu'il s'agisse d'une forme de délégation de pouvoirs de police à un acteur privé agissant sous le contrôle de l'autorité publique. Les données d'apprentissage et les modèles de fonctionnement d'un algorithme sont de fait déterminés et mis en œuvre par un acteur privé. Nonobstant le fait que la décision relèvera en définitive nécessairement de l'être humain, personne dépositaire de l'autorité publique, celui-ci peut être influencé dans sa prise de décision. Le recours à un SAAD dans le cadre de l'emploi de drones aériens de sécurité publique pourrait-il constituer un transfert partiel d'un pouvoir de police à une personne privée allant à l'encontre du principe d'interdiction de délégation fixée par la jurisprudence ? La décision du Conseil constitutionnel concernant la loi JOP 2024 introduisant l'expérimentation de caméras « augmentées » ne permet pas d'y répondre étant donné que ni les requérants ni les Sages n'ont soulevé la question d'une potentielle atteinte à l'article 12 de la DDHC[1163].

440. Au vu des évolutions jurisprudentielles depuis les années 1980 admettant que soient confiées aux acteurs privés des missions de sécurité, un constat émerge d'une tolérance par le juge des acteurs privés dans l'exercice de missions de police. L'évolution des activités de police partant d'une gestion directe pour tendre vers une supervision des acteurs (privés) chargés d'assurer des missions de sécurité ont conduit les juges à adapter leur interprétation du principe d'interdiction. Le professeur Jacques Chevallier énonçait que « c'est l'État qui trace lui-même les lignes de ce partage en fixant les attributions dont il entend se réserver l'usage exclusif et celles qu'il accepte de confier

---

[1162] Voir principalement : CE, 7e et 10e ss-sect. réunies, 1er avr. 1994, n° 144152-144241, *Commune de Menton*, *op. cit.* : « lesdites conventions ont ainsi confié à la société S. des prérogatives de police de stationnement sur la voie publique qui ne pouvaient légalement lui être déléguées ».

[1163] C. const., Décision n° 2023-850 DC, 17 mai 2023, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*, *op. cit.*, cons. 20 à 30 : Les requérants avaient contesté la durée de l'expérimentation, la carence dans la définition des évènements faisant l'objet d'une surveillance par caméras « augmentées », l'absence de garanties suffisantes aux fins d'assurer les droits et libertés sur la voie et dans les lieux publics, et la méconnaissance du principe d'égalité devant la loi.

aux autres acteurs, par un véritable processus de "délégation" »[1164]. Les modalités d'exercice du pouvoir de police mériteraient ainsi d'être redéfinies afin de ne plus faire l'objet d'éventuels écueils d'interprétation, de contentieux, ou de diviser plus sévèrement la doctrine[1165]. En ce sens, le professeur et conseiller d'État Bertrand Dacosta, constatant un déclin du principe d'interdiction de déléguer, énonçait qu' « il faudrait juger que la police administrative appartient, par nature, à l'État, […] et ceci, quelles que soient les conditions dans lesquelles la loi prévoit la participation de personnes privées. Cette affirmation […] ferait écho au principe selon lequel la police ne se délègue pas »[1166].

441. L'assouplissement de l'interprétation du principe interdisant la délégation de pouvoirs de police a permis la présence croissante du secteur privé au sein des activités régaliennes. Aussi, le recours exponentiel aux moyens technologiques de plus en plus sophistiqués n'a fait qu'amplifier ce phénomène de dépendance de l'État au secteur privé dans l'accomplissement de ses missions. Les drones aériens « augmentés » de sécurité publique s'inscrivent dans cette tendance d'une délégation des missions matérielles de police et pourraient, compte tenu de leur influence sur la décision finale[1167], conduire à une forme de délégation officieuse de pouvoirs de police au secteur privé.

§2. La dépendance croissante au secteur privé induite par les technologies « augmentées » de sécurité publique

442. Ces dernières années, les besoins en matière d'amélioration des missions de sécurité se sont essentiellement concentrés sur les nouvelles technologies qui offrent sans conteste de nombreuses opportunités. Il est désormais largement admis que l'acquisition d'informations par les agents des forces de l'ordre repose de manière significative et croissante sur le recours aux nouvelles technologies. Ces évolutions tenant à l'exercice des missions de sécurité publique, particulièrement dans le cadre des méthodes d'acquisition d'informations, ne sont cependant pas

---

[1164] CHEVALLIER (J.), « La police est-elle encore une activité régalienne ? », *Archives de politique criminelle* n° 33, vol. 1, 2011, pp. 13 à 27.

[1165] En ce sens : MOREL (B.), « L'attribution d'activités de police à des personnes privées », *op. cit.* ; PAUVERT (B.), « Le pouvoir de police ne se délègue-t-il vraiment pas ? », *op. cit.*

[1166] CE, 7ème et 2ème ss-sect. réunies, 3 juin 2009, n° 323594, *Société Aéroports de* Paris, Rec, p. 217 [en ligne].

[1167] Sur les biais d'automatisation ou biais de confiance qui incite l'être humain à accorder une confiance excessive aux résultats d'un algorithme dans sa prise de décision (précédemment évoqués) : CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 350 ; CUMMINGS (M. L.), "Automation and accountability in decision support system interface design", *op. cit.*

sans conséquence et concernent tout autant la police administrative que la police judiciaire. Or, ces technologies nécessitent un accès en réseau afin de mener les flux de données d'un endroit à un autre. Dès lors, les besoins exponentiels d'accès aux données numérisées dans le cadre des activités de police induisent *de facto* des besoins croissants d'association avec le secteur privé (A).

443. Les acteurs du secteur privé sont inscrits de longue date en tant que participants à la continuité des activités de sécurité publique. Ils agissent à des niveaux multiples dans la chaine d'information utile à l'exercice des activités des forces de l'ordre : d'une part, à des fins de services tels que l'accès aux informations, la transmission d'informations entre un outil connecté (ex. caméra de vidéoprotection) et le centre de commandement ou encore le stockage d'informations et, d'autre part, à des fins de fourniture d'outils technologiques tels que des caméras ou encore des algorithmes d'aide à la décision. Il convient de préciser que cette association du secteur privé aux activités de sécurité publique est encadrée de manière stricte. Dans le cas des opérateurs de communications électroniques, leur rôle se limite à l'interception et à la redirection des flux de données vers les services concernés[1168] assurant ainsi la confidentialité des données.

444. Pour faire face à leurs besoins, les forces de l'ordre ont eu massivement recours à deux grands types d'acteurs issus du secteur privé : des prestataires de services de sécurité[1169] (ex. stockage de données, la fourniture d'accès à un réseau, etc.)[1170] ainsi que des exploitants des réseaux de communications électroniques ou fournissant des services de communication électroniques[1171]. L'usage des nouvelles technologies par les services de police et de gendarmerie ne leur laisse d'autre alternative que d'avoir recours aux services d'entreprises spécialisées dans ce secteur. Cette situation engendre là encore des enjeux juridiques évidents tenant, cette fois, aux questions de gouvernance et de souveraineté des données traitées et stockées voire à des SAAD utilisés par les forces de l'ordre (B).

[1168] *Ibid*.

[1169] En d'autres termes, les entreprises offrant des prestations techniques destinées au milieu numérique.

[1170] Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.*, p. 48.

[1171] EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *RDP*, n°1, 1er janvier 2018, p. 189.

A. L'accès aux réseaux de communications électroniques, lien de dépendance de la force publique au secteur privé

445. L'accès aux réseaux, dont dépendent les forces de l'ordre afin d'accéder aux données nécessaires à l'exécution de leurs missions, nécessite la participation des acteurs du secteur privé. À cet effet, les opérateurs privés sont tenus de respecter des obligations spécifiques en matière de transmission des données dans le domaine tenant à la sécurité publique. L'effectivité des activités de police repose indubitablement sur la qualité des informations obtenues impliquant, entre autres, le lien de dépendance des forces de l'ordre aux entreprises fournissant un accès aux réseaux de communications électroniques. Les conséquences de cette dépendance diffèrent quelque peu selon qu'il s'agisse d'activités de police à des fins préventives ou répressives. Dans le cadre de la police administrative, les besoins d'accès aux réseaux concernent les activités liées au renseignement incluant les interceptions de sécurité[1172] (ex. interceptions de correspondances émises par voie de communications électroniques), l'accès administratif aux données de connexion[1173] ou encore la géolocalisation[1174] (ex. données techniques des équipements terminaux utilisés ou d'une caméra). Dans le cadre de la police judiciaire, ce sont les activités relatives aux interceptions judiciaires ordonnées par l'autorité judiciaire[1175] ainsi qu'à la géolocalisation d'une personne à partir d'un objet connecté en sa possession[1176] (ex. téléphone ou ordinateur) qui nécessitent un accès aux réseaux.

446. L'efficacité des activités des forces de l'ordre et des services de secours dépend par conséquent en grande partie de la qualité des réseaux issus du secteur privé. Nonobstant les réponses aux besoins que permet cette association au secteur privé, cette dépendance des activités de sécurité publique en matière de réseaux de communication peut induire de graves contraintes. L'importance de l'implication du secteur privé dans les activités régaliennes implique des atteintes potentielles à l'existence de l'État de droit en ce que celles-ci reposent entièrement sur le bon fonctionnement de ses produits et services. De ce fait, un problème technique ou une attaque informatique subie par une entreprise chargée d'une mission liée à des activités régaliennes aura des répercussions immédiates sur ces activités comme ce fut notamment le cas lors de la « panne » des

[1172] CSI, art. L. 852-1.

[1173] CSI, art. L. 851-1.

[1174] CSI, art. L. 851-4.

[1175] Code de procédure pénale (CPP), art. 100 et suiv.

[1176] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, *op. cit.* et CPP, art. 230-32 à 230-44.

numéros d'urgence[1177]. Ces difficultés peuvent avoir de graves conséquences en entrainant une suspension d'un service public dont la continuité constitue pourtant l'un des piliers fondateurs.

447. Face à ce constat, le gouvernement avait incité à la création d'alternatives permettant une meilleure gestion des réseaux de communication électronique dans le cadre des services propres à l'État tels que les services de sécurité et de secours[1178]. À cette fin le législateur a adopté la loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI) le 24 janvier 2023[1179]. Elle concrétise la volonté de renforcer les capacités numériques des services de l'État notamment en organisant la création du futur « réseau de communications électroniques des services de secours et de sécurité ». Ce réseau serait « dédié aux services publics mutualisés de communication mobile critique à très haut débit pour les seuls besoins de sécurité et de secours, de protection des populations et de gestion des crises et catastrophes »[1180]. En outre, la loi prévoit que sa mise en œuvre serait assurée directement par un opérateur public[1181] qui, toutefois, nécessitera la participation d'acteurs issus du secteur privé[1182]. Aussi, ce nouveau réseau de communication utilisera toujours les infrastructures commerciales des réseaux d'entreprises privées[1183]. Ce nouveau réseau profitera indubitablement à l'usage des drones aériens « augmentés » de sécurité publique en assurant un maintien des communications entre l'aéronef et le télépilote mais également entre les capteurs de données (ex. caméra) et le centre de commandement.

[1177] Les problèmes techniques qu'avait rencontrés la société Orange en charge du numéro d'appel d'urgence des services de sécurité civile (SAMU, Pompiers, etc.) en constitue un exemple concret. Voir notamment : DOEBELIN (V.), « Allô les secours... ? Allô ? ! », *JCP A* n° 35, 30 août 2021, act. 502 ; TRUJILLO (E.), « Panne des numéros d'urgence: la responsabilité d'Orange risque-t-elle d'être engagée ? », *Le Figaro*, 3 juin 2021 [en ligne] ; « La panne des numéros d'urgence causée par un « bug » logiciel, selon l'enquête interne d'Orange », *Le Monde*, 11 juin 2021 [en ligne].

[1178] Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, « Panne des numéros d'urgence : le Gouvernement annonce des premières mesures », 22 juillet 2021 [en ligne] ; Vie publique, « Panne des numéros d'urgence : quelle responsabilité de l'opérateur Orange ? », 29 juillet 2021 [en ligne] consultés le 7 avril 2023.

[1179] Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI), *JORF* n°0021 du 25 janvier 2023 [en ligne].

[1180] LOPMI, art. 11 : aussi désigné sous les termes de « réseau radio du futur » ou RRF.

[1181] CPCE, art. 15 ter nouveau : Ce nouveau réseau numérique sera mis en œuvre par un « établissement public chargé d'assurer le service public d'exploitation du réseau de communications électroniques des services de sécurité et de secours ».

[1182] CHEMINAT (J.), « Le ministère de l'Intérieur lance le chantier de son futur réseau radio 4G/5G », *Le Monde Informatique*, 14 octobre 2022 [en ligne] ; THIERRY (G.) « Ce que le « réseau radio du futur » va changer pour les sapeurs-pompiers », *La Gazette des communes*, 12 décembre 2022 [en ligne] consultés le 7 avril 2023.

[1183] KARAYAN (R.), « Coup d'envoi pour le "réseau radio du futur", opérationnel en 2024 », *L'Usine Digitale*, 13 octobre 2022 [en ligne] consulté le 7 avril 2023.

448. Les drones aériens « augmentés » de sécurité publique requièrent un accès permanent aux réseaux de communication électronique (afin de transmettre les données collectées) ainsi qu'à des fréquences radio afin de piloter le drone. Dès lors, ils participent à cette dépendance aux acteurs privés issus du secteur du numérique, à l'instar d'autres systèmes de vidéoprotection. Outre les réseaux de communication, la dépendance des activités de police réside également dans les outils servant au traitement des données collectées dont la conception dépend du secteur privé.

B. Les technologies de traitement de données policières, outils de coproduction de sécurité publique

449. S'agissant des données policières, les entreprises privées du secteur numérique jouent un double rôle par l'accès à des données exploitables et la classification des données utiles aux forces de l'ordre afin d'obtenir des informations. Le traitement des données de la police administrative du renseignement échappe à l'intervention des acteurs du secteur privé qui dépend presque exclusivement du Groupement interministériel de contrôle concernant le recueil, la centralisation et la conservation des données, et ce quelle que soit la technique de renseignement utilisée[1184]. À l'inverse, le secteur privé occupe une place prépondérante concernant les données destinées à la police judiciaire par l'intermédiaire de la plateforme nationale des interceptions judiciaires introduite par le décret n° 2014-1162 du 9 octobre 2014[1185]. Néanmoins, celle-ci a subi des critiques résultant de plusieurs difficultés d'ordre technique ayant pour conséquence d'en faire un outil peu efficace et vulnérable aux attaques informatiques.

450. Aussi, les acteurs du secteur privé fournissent des solutions en matière de gestion de données massives (*Big data*). Les forces de l'ordre disposent d'un arsenal d'outils technologiques leur permettant de collecter un nombre important de données[1186]. Cependant, le volume de données collectées présente de lourds inconvénients d'exploitation qui nécessite un « tri » complexe de celles-ci afin d'extraire des informations exploitables et pertinentes à l'usage des forces de l'ordre.

[1184] CSI, art. R. 823-1.

[1185] Décret n° 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plateforme nationale des interceptions judiciaires », *JORF* n°0236 du 11 octobre 2014 [en ligne].

[1186] À cette fin, le législateur a mis en œuvre plusieurs dispositions permettant l'exploitation de données massives. Elle est permise aux services de police administrative par la loi n° 2015-912 relative au renseignement du 24 juillet 2015 et la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (*JORF* n°0278 du 1 décembre 2015 [en ligne]) et aux services de police judiciaire, principalement, par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale (*JORF* n°0129 du 4 juin 2016 [en ligne]).

Cette opération requière l'intervention d'acteurs du secteur privé dans la conception d'outils permettant le traitement de ces données.

451. Il est incontestable que l'exécution des missions des forces de l'ordre et des services de secours dépend massivement du secteur privé issu du domaine des hautes technologies dans l'objectif d'accroitre la quantité d'informations[1187]. Les forces de l'ordre et, dans une moindre mesure, les services de secours sont aujourd'hui largement tributaires des technologies du secteur privé permettant la classification des données qu'ils collectent. Cependant, cette dépendance au secteur privé engendre des enjeux de souveraineté. En ce sens, l'analyse des données issues de la lutte contre le terrorisme menée par la Direction générale de la Sécurité intérieure (DGSI) a longtemps requis l'utilisation de systèmes encore inexistants en France obligeant *de facto* les autorités publiques à confier le traitement de ces données à la société américaine *Palentir*[1188]. Cette « co-gestion » de la sécurité publique par les forces de l'ordre et le secteur privé prête à controverse et suggère une remise en question des principes tenant à la souveraineté des activités de police. En outre, la gestion externalisée des données de police induit un transfert de la gestion d'une partie des cybermenaces sur ces données au secteur privé.

452. En outre, l'attribution de l'analyse de données de police à une entreprise étrangère suppose qu'une part de contrôle lui est octroyée ce qui amplifie les enjeux de souveraineté à l'inverse d'une attribution de cette gestion à une entreprise privée nationale. Aussi, le fait que cette entreprise soit d'origine étrangère amplifie la complexité de contrôle tant concernant la protection des droits des personnes concernées vis-à-vis de leurs données que concernant la sécurité de ces données. L'emploi d'outils technologiques et de services issus du secteur privé dans le cadre d'activités de police est soumis à un encadrement strict qui suppose notamment le maintien du principe de souveraineté. Pourtant, dans le cas de la délégation de l'exploitation de données à l'entreprise américaine *Palentir*, il est incontestable qu'il existe une délégation d'activités de police par le traitement des données fournies par la DGSI. Cette délégation n'est en soit pas contraire aux principes constitutionnels français mais soulève néanmoins la question du contrôle effectif du

---

[1187] VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.* : « L'atout principal du ministère de l'Intérieur est […] la connaissance d'un certain nombre d'informations intéressant la sécurité intérieure. Avec les nouvelles, technologies, ces informations sont disponibles grâce au *Big data* et sont exploitables grâce aux algorithmes d'IA » (p. 11) dont « le monopole est détenu par les entreprises privées » (p. 115) ; EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *op. cit.*

[1188] EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *op. cit.*

pouvoir régalien sur le traitement de données relevant du domaine pénal à une entreprise étrangère.

453. Le Sénat a eu l'occasion de réitérer l'importance d'assurer la souveraineté technologique française et européenne[1189]. Il a appelé à mettre en œuvre un cadre juridique en matière de technologies basées sur des algorithmes d'IA dans les plus brefs délais afin de ne pas brider l'innovation française et européenne dans ce domaine et d'apporter de fortes garanties assurant une protection effective des droits et libertés. L'élaboration d'un cadre juridique adapté permettrait ainsi de parer au recours par « les acteurs publics et privés [à] des solutions développées à l'étranger, avec des niveaux de contraintes bien moindre »[1190] .

454. Outre l'enjeu de souveraineté, le fait d'avoir recours à des algorithmes permettant d'analyser des données collectées par un système de vidéoprotection, conçus par des entreprises privées, afin d'aider les forces de l'ordre dans leur prise de décision suggère une possible délégation de pouvoirs de police au secteur privé. Dès lors, le recours à des algorithmes dans le processus décisionnel des forces de sécurité publique remet en question le caractère régalien de la force publique. L'insertion du secteur privé au sein des activités de sécurité publique laisse craindre une opposition décisionnelle entre les « règles » algorithmiques établies par leurs concepteurs et les règles émanant des textes nationaux et supranationaux qui défendent les droits et libertés.

455. Le recours à des SAAD suggère une limitation de la liberté individuelle dans le sens où la possibilité d'une décision arbitraire ne résulte plus uniquement de l'État mais pourrait reposer pour une part sur une conception biaisée du logiciel par une entreprise privée. Aussi, ce « pouvoir » de participation de l'algorithme dans la prise de décision, sur lequel l'État ne dispose d'aucun contrôle, s'oppose dès lors au principe interdisant la délégation de pouvoirs de police dérivée de l'article 12 de la DDHC et de la jurisprudence du Conseil constitutionnel. En ce sens, l'absence, même partielle, de contrôle du pouvoir régalien sur les critères servant aux calculs effectués par l'algorithme dont les résultats participent au processus décisionnel des agents des forces de l'ordre constitue une délégation partielle du pouvoir de police à des entreprises privées.

[1189] Sénat, Rapport d'information n°627 (2021-2022) sur « La reconnaissance faciale et ses risques au regard de la protection des libertés individuelles » remis par DAUBRESSE (M-P.), de BELENET (A.) et DURAIN (J.), 10 mai 2022, *op. cit.*, pp. 102 et suiv.

[1190] *Idem*, p. 8.

456. Afin de pallier cette absence partielle de contrôle de l'État sur les technologies auxquelles elle a recours, l'agence nationale pour la recherche supervise la création de nombreux projets impliquant des industriels, des universitaires et les autorités publiques. Néanmoins, l'enjeu semble subsister du fait d'une insuffisance d'implication concrète des forces de l'ordre pour le développement de ces technologies[1191]. Pourtant, le contrôle des « règles » régissant le fonctionnement de l'algorithme de même que la maitrise des connaissances de son fonctionnement sont essentiels. Dès lors, le recours à des algorithmes dans le cadre d'activités de police fait face à un défaut de connaissance et de formation des autorités publiques quant au mode de conception et d'utilisation de leurs algorithmes. De manière similaire, les agents habilités à l'utilisation d'outils de vidéoprotection avaient pâtis d'un manque de formation leur permettant de maîtriser pleinement le fonctionnement de ces outils[1192]. En matière d'activités de police, les agents des forces de l'ordre devraient rencontrer des difficultés semblables avec les algorithmes et ce principalement s'agissant des algorithmes plus récents qui devraient être à la fois plus performants et adaptés mais aussi plus complexes.

457. D'une manière générale, le fait de confier certaines activités de police au secteur privé participe à la remise en question de l'État de droit qui repose sur des valeurs démocratiques impliquant *de facto* les citoyens. Or, les algorithmes développés par des entreprises issues du secteur privé n'entrent pas dans ce processus démocratique lorsque l'État n'est pas effectivement impliqué dans leur processus de conception. Concrètement, il n'existe aucune garantie permettant d'établir de manière effective que les valeurs et principes qui régissent l'entreprise conceptrice des algorithmes pouvant être associés à des drones aériens de sécurité publique reflètent ceux de l'État et qui reposent sur les textes nationaux et supranationaux protégeant les droits et libertés.

Section 2 Les drones aériens « augmentés » de sécurité publique : outils d'une pérennisation de l'État d'exception ?

458. Depuis de longues années, des chercheurs cherchent à élaborer des modèles reposant sur les mathématiques et les algorithmes afin de résoudre les problèmes et suggérer des solutions

---

[1191] Les forces de l'ordre (lorsqu'elles sont impliquées directement) ne sont pas toujours présentent lors des réunions - y compris finales - détaillant les travaux et les développements technologiques effectués dans le cadre des projets de recherche impliquant les universitaires et les industriels. Cf. projet FUI COOPOL et projet ANR GIRAFE.

[1192] Voir en ce sens, l'étude produite par Élodie Lemaire sur les caméras de vidéoprotection : LEMAIRE (É.), *L'oeil sécuritaire : Mythes et réalités de la vidéosurveillance*, *op. cit.*

adaptées en vue d'améliorer l'exécution des tâches dans différents domaines d'activités qu'ils soient économiques, énergétiques, agricoles ou encore industriels. Certains modèles semblent apporter des solutions satisfaisantes dans certains domaines tels que dans la gestion de l'énergie, à l'image du modèle Optimum développé par le mathématicien Jean-Bernard Lasser[1193]. Nonobstant les résultats concluants de son modèle et l'omniprésence de ce type de technologies dans notre quotidien, Monsieur Lasser émet des réserves quant à leur adaptabilité à certains domaines tels que la sociologie ou la science politique. Ainsi, il considère que « pour tout domaine d'activité où les actions et les relations humaines peuvent être chiffrables ou mises en statistique, il est tout à fait possible de poser un problème d'optimisation avec un modèle mathématique. Pour le reste, on se gardera bien de modéliser le libre arbitre »[1194].

459. Pourtant, le pari de faire usage de caméras de surveillance « augmentées » à des fins de détection voire d'anticipation d'évènements est déjà lancé[1195]. L'identification d'évènements « prédéterminés » comme présentant un risque pour la population, à l'aide d'un algorithme d'analyse d'images associé à des systèmes de vidéoprotection, se présente comme une avancée majeure dans l'exercice des missions de sécurité publique. Outre l'objectif dissuasif que peuvent potentiellement accroitre les drones aériens (« augmentés » ou non) de sécurité publique, ceux-ci sont susceptibles de participer à l'établissement de la preuve dans le cadre du procès pénal. Cependant, l'emploi à cette fin des drones aériens de sécurité publique associés à des algorithmes « augmentés » pourrait venir redéfinir le caractère de la preuve dans le cadre du procès pénal (§1) et avoir une incidence conséquente sur l'État de droit (§2).

§1. Le renouvellement de la preuve pénale par les drones aériens « augmentés » de sécurité publique

460. Face au contexte de croissance des incivilités et des besoins en matière de lutte contre la criminalité organisée et le terrorisme, le législateur a entrepris de renforcer les compétences et les

---

[1193] Voir à ce sujet l'article de NIKITINE (K.), « Mathématiques : À la recherche du meilleur des mondes », *Sciences & Vie* n° 1260, septembre 2022, pp. 98-101.

[1194] *Idem*, p. 101 : citation de LASSER (J-B.) Mathématicien et directeur de recherche émérite du CNRS.

[1195] Voir en ce sens : Loi JOP 2024 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.* ; Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.* ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

moyens mis à la disposition des autorités publiques. La loi RPSI participe ainsi à ce renforcement en autorisant le recours à des drones aériens par les forces de l'ordre. Ce faisant, le législateur introduit de nouveaux outils d'aide à l'établissement de la preuve dans le cadre d'un procès pénal (A). Cependant, le couplage d'algorithmes d'analyse d'évènements à des systèmes de vidéoprotection, tels que les drones aériens, ne représente pas qu'un nouveau moyen mis en œuvre à l'appui des forces de l'ordre mais transforme la nature de la surveillance de la voie publique[1196]. Dès lors, les caméras de surveillance « augmentées » introduisent une nouvelle forme d'établissement de la preuve pénale au travers de l'analyse des données qu'elles effectuent préalablement à la prise de décision finale des forces de l'ordre (B).

A. Les conditions d'admissibilité de la preuve pénale issue des drones aériens de sécurité publique

461. La manifestation de la vérité constitue un élément capital du procès pénal[1197]. Aussi, la qualification de preuve[1198] n'est pas sans conséquence en ce qu'elle permet de mettre en cause la liberté des personnes contre lesquelles elle s'oppose[1199]. Dès lors, tout élément recueilli par un drone aérien de sécurité publique devra revêtir la qualification de preuve avant de pouvoir être présenté dans le cadre d'une procédure pénale. En droit pénal, la preuve recueillie par une autorité publique est soumise au respect de deux principes que sont la liberté et la licéité de la preuve[1200]. Le principe de liberté de la preuve suppose la recherche et la production devant un juge de tous les éléments permettant la découverte de la vérité par les autorités publiques, d'une part, et la liberté d'appréciation des preuves par le juge qui statue sur base de son intime conviction, d'autre part (1). Néanmoins, cette liberté est limitée par le principe de licéité de la preuve qui exige que « la

---

1196 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 12.

1197 VERGÈS (É.), *Procédure pénale*, Paris, LexisNexis, 6ème édition, 2020, 388 p., p. 83.

1198 D'une manière générale, la preuve constitue une démonstration de la véracité d'un ou de plusieurs faits.

1199 DANJAUME (G.), « Le principe de la liberté de la preuve en procédure pénale », *Rec. Dalloz* n° 18, 2 mai 1996, p.153 : « En procédure pénale, la preuve revêt une importance toute particulière dans la mesure où elle va permettre de statuer sur la culpabilité ».

1200 ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, Paris, Vuibert, 12ème édition, 2021, 480 p., p. 185 : « Cette liberté [de la preuve pénale] connait des limites tenant à la légalité ainsi qu'à la loyauté » ; VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 88 : « Pour éviter que cette liberté [de la preuve pénale] ne s'exerce au détriment des droits des parties, le Code de procédure pénale et la jurisprudence imposent que cette preuve soit recherchée de façon licite » ; BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », 2020, n° 48 : « Ce principe de la liberté de la preuve doit forcément se concilier avec un autre principe, fondamental, celui de la légalité à laquelle se trouve nécessairement soumise la preuve qui doit être administrée, au premier chef, par des agents de la puissance publique ».

recherche, la production et l'appréciation des preuves pénales doivent se faire conformément au droit »[1201] ; en d'autres termes, qu'elle ne contrevienne pas à l'ordre public ainsi qu'aux bonnes mœurs (2).

1. Le principe de liberté de la preuve appliqué aux drones aériens de sécurité publique

462. La procédure pénale se fonde principalement sur le principe de liberté de la preuve[1202] qui dispose que : « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve »[1203]. Ainsi, la liberté de la preuve suppose l'admissibilité de tous les modes de preuve[1204] (a). En matière pénale, l'appréciation de la preuve ne repose donc que partiellement sur le principe de la preuve légale[1205] car son champ est réduit par le principe de l'intime conviction[1206]. Dès lors, le juge demeure libre de rendre sa décision en se référant à tout autre moyen de preuve pour établir la culpabilité ou l'innocence du prévenu selon son intime conviction[1207] (b).

a. La recevabilité des preuves issues des drones aériens de sécurité publique

463. Le principe de la liberté de la recherche et de production de la preuve s'applique à toutes les autorités publiques et est affirmé tant par la législation que par la jurisprudence[1208]. En ce sens,

---

[1201] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 88 ; CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 552.

[1202] SONTAG KOENIG (S.), *Technologie de l'information et de la communication et défense pénale*, Paris, Mare & Martin, Thèse, 2015, 744 p., p. 176 : « La procédure pénale est profondément imprégnée d'un principe de liberté de la preuve (art. 427 CPP), dans l'admission de cette dernière mais également dans la faculté du juge de la recevoir ou non » ; BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », *op. cit.*, n° 49.

[1203] CPP, art. 427, al. 1er.

[1204] Elle peut être définie comme « ce qui, en vertu de la loi, peut être proposé en preuve par un plaideur au soutien de ce qu'il allègue, de telle sorte que le juge est tenu de prendre en considération, sans pouvoir l'écarter *a priori,* la preuve offerte, mais sans être certain que celle-ci soit reconnue apte, après examen, à justifier l'allégation » (CORNU, (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 31).

[1205] Toutefois, le droit français semble avoir majoritairement abandonné le système de la preuve légale (ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 185) qui a longtemps prévalu au cours de l'Histoire (LAINGUI (A.) et LEBIGNE (A.), *Histoire du droit pénal : La procédure criminelle*, Paris, Cujas, Tome II, 1979 ; CARBASSE (J-M.), *Histoire du droit pénal et de la justice criminelle*, Paris, PUF, 2000, 445 p.).

[1206] ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 189 ; VERGÈS (É.), *Procédure pénale*, *op. cit.*, pp. 85-86.

[1207] C. cass., ch. crim., 24 janvier 1973, n° 72-90.691 [en ligne].

[1208] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 84 : « La liberté de chercher et de produire la preuve se manifeste à tous les stades de la procédure et pour toutes les autorités publiques ».

le CPP attribue aux officiers de police judiciaire le pouvoir « de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs »[1209]. Ce principe est également rappelé par la jurisprudence dans un arrêt de la Cour de cassation du 11 juin 2004 où les juges ont estimé que « les autorités judiciaires [sont] tenues de procéder à tous actes utiles à la manifestation de la vérité »[1210]. En outre, le principe de liberté de la preuve n'impose aucune hiérarchie entre les types de preuves ; en d'autres termes, aucune preuve n'est juridiquement supérieure à une autre et il revient au juge, selon son intime conviction, de déterminer les preuves les plus convaincantes[1211].

464. L'introduction de nouvelles technologies à l'usage des forces de l'ordre a contribué à la diversification des formes de preuves en matière pénale[1212]. Aujourd'hui, la procédure pénale comporte de nombreux moyens technologiques permettant le recueil de la preuve[1213]. Le législateur a progressivement autorisé cet élargissement des modes de preuve afin d'octroyer des moyens suffisants aux autorités publiques dans leurs missions d'établissement des faits. Aujourd'hui, les capacités de collecte de données des drones aériens de sécurité publique présentent un intérêt capital pour les forces de l'ordre dans la mesure où ces images pourraient potentiellement revêtir le caractère d'éléments probatoires. Certains affirment que « les technologies offrent de nouvelles perspectives aux enquêteurs [et] le crédit apporté à un enregistrement sonore et plus encore à une bande magnétique[1214] est souvent bien supérieur car sans risque de subjectivité »[1215]. Ainsi, l'enregistrement d'images participe à l'établissement des faits en apportant des éléments objectifs dans le cadre d'une procédure pénale[1216]. En d'autres termes, ce procédé s'accorde avec le principe de liberté de la preuve du procès pénal qui tend à la manifestation de la vérité.

[1209] CPP, art. 14.

[1210] C. cass., ass. plén., 11 juin 2004, n° 98-82.323 [en ligne] et cf. CPP, art. 310.

[1211] ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 189 ; VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 85.

[1212] COMMARET (D.), « Les métamorphoses de la preuve pénale », *Revue pénitentiaire* n° 4, 2003, pp. 735-744.

[1213] FERAL-SCHUHL (C.), « La collecte de la preuve numérique en matière pénale », *AJP* n° 3, 2009, p. 115 : « les méthodes d'investigations se sont [...] adaptées et ajustées grâce aux nouvelles technologies de l'information et de la communication ».

[1214] En d'autres termes, un enregistrement vidéo.

[1215] VITALIS (A.), « Vidéosurveillance et libertés individuelles », *Revue de la gendarmerie nationale* n° 199, 2ème trimestre 2001, p. 25.

[1216] *Idem* : « L'objet représenté s'imprimant directement sur la couche sensible de la pellicule, l'image vidéo constitue une preuve, un certificat de réalité. Plus qu'une représentation, il s'agit d'une présentation ».

465. L'emploi de caméras filmant la voie publique est admis comme étant un moyen recevable de collecte de preuves pénales par enregistrement d'images[1217]. Ce mode de preuve est spécifié dans les textes et prévu par le CSI dans le cadre des activités de police administrative[1218] ainsi que par le CPP dans le cadre des activités de police judiciaire[1219]. En pratique, lorsqu'une infraction a été signalée, les forces de l'ordre peuvent demander à ce que les vidéos pouvant leurs être utiles leurs soient communiquées et dresser un procès-verbal[1220], s'il y a lieu, après leur visionnage. La législation exige de ne mentionner dans le procès-verbal que « les données enregistrées qui sont utiles à la manifestation de la vérité »[1221]. Ce procès-verbal peut alors être déposé en tant que preuve dans le cadre du procès pénal.

466. Les juges de la chambre criminelle de la Cour de cassation admettent ce mode de preuve comme étant recevable lors des débats[1222] (en vertu du principe du contradictoire) sous réserve que les images aient été collectées dans le respect des principes relatifs au procès pénal (v. **n° 471 et suiv.**). Les forces de l'ordre peuvent aujourd'hui procéder à des enregistrements d'images par drones aériens à des fins de recherche de preuve des infractions ou même dans le cadre d'une enquête judiciaire[1223] après autorisation et sous le contrôle du procureur de la République[1224]. Dans ces conditions, les images collectées par une caméra de vidéoprotection (fixe ou mobile) sont recevables à titre de preuve par le juge pénal[1225]. Une preuve par enregistrement d'images de la voie publique peut ainsi être reconnue comme admissible mais devra néanmoins toujours répondre au principe du contradictoire et sa force probante relève de l'appréciation du juge pénal.

467. Par ailleurs, ce mode de preuves est admis par la CEDH qui considère l'utilisation d'enregistrements d'images portant sur des individus effectués sur la voie publique comme n'étant

---

[1217] VERGÈS (E.), VIAL (G.) et LECLERC (O.), *Droit de la preuve*, Paris, PUF, 2ème édition, 2022, 828 p., p. 714.

[1218] CSI, art. L. 252-1 (caméras fixes) et art. L. 242-5 (caméras aéroportées)

[1219] CPP, art. 81.

[1220] CPP, art. 230-38.

[1221] CPP, art. 230-39.

[1222] C. cass., ch. crim., 9 janvier 2018, n° 17-82-946 [en ligne].

[1223] Les juges de la Cour de cassation ont accordé au procureur « le pouvoir de faire procéder, sous son contrôle effectif et selon les modalités qu'il autorise s'agissant de sa durée et de son périmètre à une vidéosurveillance sur la voie publique aux fins de rechercher la preuve des infractions à la loi pénale » (C. cass., ch. crim., 8 décembre 2020, n° 20-83.885 [en ligne]).

[1224] CPP, art. L. 230-48 1°.

[1225] C. cass., ch. crim., 11 décembre 2018, n° 18-82.365, *op. cit.* ; C. cass., ch. crim., 18 juin 2019, n° 18-86.421, *op. cit.*

pas contraire au droit au respect de la vie privée[1226]. En ce sens, elle distingue « la surveillance des actes d'un individu dans un lieu public à des fins de sécurité des enregistrements de ces actes qui seraient utilisés à d'autres fins allant au-delà de ce que l'intéressé aurait pu prévoir »[1227]. Dès lors, les images d'individus prises dans des lieux publics par des drones aériens de sécurité publique pourront être reconnues comme admissibles à titre de preuve dans le cadre d'une procédure judiciaire[1228]. Pour autant, la recevabilité des preuves dépend de l'appréciation du juge qui agit selon son intime conviction.

b. La liberté d'appréciation des preuves issues des drones aériens de sécurité publique par le juge

468. Le juge est libre d'apprécier la valeur des preuves qui lui sont présentées selon le principe de l'intime conviction[1229]. En d'autres termes, les juges apprécient librement la culpabilité de la personne présentée devant eux à l'appui des preuves qui leurs sont présentées[1230]. En ce sens, le fait que des éléments de preuve soient recueillis par l'intermédiaire de moyens technologiques, tels que des drones aériens de sécurité publique, ne leur confère aucunement un statut probatoire irrévocable. Dès lors, les images collectées par des dispositifs de vidéoprotection doivent faire l'objet d'un examen par le juge pénal au même titre que tout autre élément servant à établir la vérité. Aussi, la Cour de cassation admet un pouvoir souverain des juges du fond quant à l'appréciation des faits et des preuves soumis[1231].

[1226] CEDH, 25 septembre 2001, *P.G. et J.H. c. Royaume-Uni,* n° 44787/98, §56 [en ligne].

[1227] CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, *op. cit.*, § 57 et CEDH, 20 décembre 2005, *Wisse c. France*, n° 71611/01, § 26 [en ligne].

[1228] CPP, art. 230-47 et suiv. ; SIBER (J.), « L'image et le manifestant », *Gaz. Pal.* n°4, 24 janvier 2017, p. 81.

[1229] CPP, art. 427 : « le juge décide d'après son intime conviction ».

[1230] HELIE, *Traité d'instruction criminelle*, Tome IV, Plon, 2ème édition, 1886, 708 p., n° 1780 : « Toutes les preuves, quelle que soit leur nature […] sont simplement offertes à l'appréciation du juge, qui est libre de puiser son opinion aussi bien dans une preuve négative, conjecturale et imparfaite, que dans une preuve affirmative, directe et complète ».

[1231] Voir notamment : C. cass., ch. crim., 4 juin 1991, n° 91-81.682 [en ligne] ; C. cass., ch. crim., 4 juin 1998, n° 96-85.871 [en ligne] ; DANJAUME (G.), « Le principe de la liberté de la preuve en procédure pénale », *op. cit.*, p.153.

469. La décision du juge doit reposer sur examen approfondi des preuves qui lui auront été soumises lors des débats et conformément au principe du contradictoire[1232]. À cette fin, le juge devra respecter une double obligation de cohérence et de motivation de sa décision sous peine de nullité[1233]. Cette obligation de motivation suppose que les juges expliquent les raisons qui les ont menées à prendre leur décision[1234] dans le respect du droit au procès équitable formulé par la Conv.EDH[1235]. Cette condition permet d'assurer un contrôle de la décision afin de vérifier que « les juges n'ont pas commis d'erreur dans l'appréciation qu'ils ont portée sur ces faits »[1236]. En ce sens, l'obligation pour le juge de devoir motiver sa décision est une garantie au respect de la présomption d'innocence[1237].

470. Aussi, le principe de l'intime conviction n'induit pas une décision arbitraire reposant sur une appréciation approximative des juges mais, à l'inverse, suppose que les juges rendent leur décision en ayant la certitude de la culpabilité ou de l'innocence de la personne inculpée[1238]. Dès lors, le doute doit profiter à la personne poursuivie qui ne peut se voir condamner par les juges[1239]

[1232] Le principe du contradictoire est une des déclinaisons du droit au procès équitable énoncé à l'article 6 § 3 de la Conv.EDH. Il est essentiel à la procédure pénale et s'impose à toutes les parties au procès. De manière synthétisée, la CEDH a défini le principe du contradictoire comme « la faculté pour les parties à un procès pénal ou civil, de prendre connaissance de toutes les pièces ou observations présentées au juge, même par un magistrat indépendant, en vue d'influencer sa décision et de la discuter » (CEDH, 20 février 1996, *Vermeulen c. Belgique*, n° 19075/91, § 33 [en ligne]).

[1233] CPP, art. 485 : Le jugement doit comprendre les motifs qui « constituent la base de la décision ».

[1234] Le professeur Gérard Cornu décrit l'obligation du juge de justifier sa décision comme « le fait pour un juge de fonder sa décision en fait et en droit, en la motivant suffisamment pour lui donner une base légale » (CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 533) ; RENUCCI (J-F.), « Intime conviction, motivation des décisions de justice et droit à un procès équitable », *Recueil Dalloz*, 2009, p. 1058 : La motivation de la décision du juge pénal a été établie comme une garantie du procès équitable « car elle permet de préserver les droits de la défense […] indispensable à la qualité même de la justice et […] rempart contre l'arbitraire ».

[1235] Conv.EDH, art. 6, §§ 1 et 2 ; CEDH, 19 avril 1994, *Van de Hurk c. Pays Bas*, n° 16034/90, § 61 [en ligne] : « l'article 6 par. 1 (art. 6-1) oblige les tribunaux à motiver leurs décisions, mais il ne peut se comprendre comme exigeant une réponse détaillée à chaque argument » ; CEDH, 19 décembre 1997, *Helle c. Finlande*, n° 20772/92, §60 [en ligne] : « la notion de procès équitable requiert qu'une juridiction interne qui n'a que brièvement motivé sa décision […] ait réellement examiné les questions essentielles qui lui ont été soumises et qu'elle ne se soit pas contentée d'entériner purement et simplement les conclusions d'une juridiction inférieure ».

[1236] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 86.

[1237] BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », *op. cit.*, n° 13 : Le principe de la présomption d'innocence est consacré à l'article 9 de la DDHC qui lui confère le statut de principe fondamental et énoncé à l'article 9-1 du Code civil. Ce principe est également reconnu à l'article 6 §2 de la ConvEDH. De même l'article préliminaire du CPP énonce que « toute personne suspectée ou poursuivie est présumée innocente tant que sa culpabilité n'a pas été établie. Les atteintes à sa présomption d'innocence sont prévenues, réparées et réprimées dans les conditions prévues par la loi ». Enfin, il est inscrit à l'article 48 de la CDFUE et a fait l'objet d'un renforcement par la Directive (UE) 2016/343 sur la présomption d'innocence du 9 mars 2016, *JOUE* n° L 65, 11 mars 2016 [en ligne].

[1238] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 86.

[1239] Cependant, en pratique, il se peut que le juge soit convaincu par certains éléments sans nécessairement avoir la certitude de la culpabilité de la personne inculpée (ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 181).

selon l'adage *in dubio pro reo*. Si le droit pénal admet le principe de la liberté de la preuve cela ne la soustrait pas à l'application de règles de droit. En d'autres termes, la recherche et la production de preuves doivent être conformes au droit en respectant les dispositions législatives et la jurisprudence qui imposent que ces preuves soient collectées de manière licite.

2. Les exigences à l'admissibilité des preuves issues des drones aériens de sécurité publique

471. Le droit de la preuve pénale repose sur le respect de plusieurs exigences qui relèvent du principe de licéité de la preuve. Celui-ci suppose l'interdiction des preuves illégales, illicites ou déloyales. Dès lors, le processus de collecte de données par les drones aériens de sécurité publique doit respecter les règles de droit afin que les informations collectées puissent être recevables dans l'éventualité d'une procédure pénale. La preuve devra donc être recueillie de manière licite. Cela suppose pour les forces de l'ordre de respecter l'obligation d'obtenir une autorisation préalable de l'autorité compétente afin de recourir à des drones aériens ainsi que la remise à la CNIL d'une analyse d'impact sur la protection des données. Aussi, il convient de préciser que certains modes de preuves sont soumis à un cadre législatif précis.

472. Afin de faire face aux infractions les plus graves, le législateur a également introduit des dispositions entrant dans le cadre des procédures pénales dérogatoires qui incluent notamment le recours à des technologies de traitement et d'analyse de données. Il en va ainsi des procédures de géolocalisation[1240] ou encore du recours à des dispositifs de captation d'images dans des lieux privés par les forces de l'ordre à des fins d'enquête[1241]. Ces procédures pénales exceptionnelles se sont multipliées de manière exponentielle s'agissant des infractions les plus sérieuses au rang desquelles

[1240] CPP, art. 230-32 et suiv. : La législation autorise la géolocalisation en temps réel à des fins d'enquête.

[1241] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, *JORF* n°59 du 10 mars 2004 [en ligne] ; L'article 706-96 du CPP admet les méthodes d'investigation qui autorisent « la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement […] de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé ». Dernièrement, le procédé de captation d'images dans des lieux privés par les officiers de police judiciaire, sans le consentement des personnes concernées, a été étendu aux drones aériens de sécurité publique (C. cass., ch. crim., 15 novembre 2022, n° 22-80.097 [en ligne]). L'affaire concernait une opération de captation d'images sur la propriété du défendeur à des fins d'enquête concernant le trafic de stupéfiants.

se trouvent la criminalité organisée et le terrorisme[1242]. Au regard du caractère particulièrement intrusif pour la vie privée, ces mesures pénales dérogatoires font l'objet d'un encadrement strict par le législateur qui les limite aux seules infractions relevant de la criminalité organisée[1243] regroupées au sein des « techniques spéciales d'enquête »[1244] du CPP depuis la loi du 23 mars 2019[1245].

473. Aussi, la licéité de la preuve pénale ne repose pas uniquement sur le respect des règles de droit. Plusieurs garanties ont été édifiées afin de protéger les personnes contre des décisions arbitraires prises par l'État à leur encontre. Ainsi, les autorités publiques ne peuvent outrepasser leurs autorisations légales inscrites dans le CPP et, par conséquent, procéder à la collecte d'éléments probatoires en commettant une infraction[1246]. En ce sens, les forces de police judiciaire ne pourraient collecter des images de l'intérieur du domicile d'un individu au moyen de drones aériens sans autorisation préalable de l'autorité judiciaire compétente.

474. En outre, la licéité de la preuve suppose le respect des droits de la défense qui incluent la loyauté de la preuve, le principe du contradictoire, la protection de l'intimité de la vie privée ou encore la présomption d'innocence[1247]. Le principe de loyauté de la preuve n'apparait pas dans le CPP mais est depuis longtemps admis par la jurisprudence[1248]. Il interdit d'avoir recours à des procédés déloyaux, de ruse ou à de stratagèmes notamment à des fins de constatation d'une infraction[1249]. Aussi, ce principe mérite d'être abordé s'agissant du recours à des drones aériens à

[1242] THOMAS-TAILLANDIER (D.), *Contribution à l'étude des procédures dérogatoires*, Aix en Provence, Presses Universitaires d'Aix-Marseille, Thèse, 2014, 423 p., p. 50. À titre d'exemple : Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, *JORF* n°0075 du 29 mars 2014 [en ligne] ; Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n°0171 du 26 juillet 2015 [en ligne] ; Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, *op. cit.*

[1243] Ces infractions sont listées aux articles 706-73 et 706-73-1 du CPP.

[1244] Les techniques spéciales d'enquête sont les actes d'investigation les plus intrusifs. Sur le sujet voir notamment : GUINCHARD (S.) et BUISSON (J.), *Procédure pénale*, *op. cit.*, p. 789 et suiv. ; PARIZOT (R.), « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique » *in* PELLÉ (S.) (dir.), *Quelles mutations pour la justice pénale du XXIe siècle ? À partir de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme de la justice*, Paris, Dalloz, coll. Thèmes et commentaires, 2020, 296 p., p. 71.

[1245] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme de la justice, *JORF* n°0071 du 24 mars 2019 [en ligne].

[1246] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 94.

[1247] BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », *op. cit.*, n° 175 et n° 203.

[1248] C. cass., ch. crim., 12 juin 1952.

[1249] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 88 ; BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », *op. cit.*, n° 180.

des fins de captation d'images dans la mesure où cette technique est reconnue comme étant particulièrement intrusive[1250] et que ces aéronefs peuvent s'avérer particulièrement discrets. Aussi, la licéité de la preuve implique de respecter le droit à la protection de la vie privée[1251]. Dès lors, les preuves collectées au moyens de drones aériens de sécurité publique ne peuvent être licites que si l'atteinte qu'ils portent à ce droit est strictement prévue par la loi, repose sur un objectif légitime, est nécessaire à la manifestation de la vérité et proportionné[1252]. Enfin, le principe de licéité de la preuve suppose le respect du principe du contradictoire[1253] qui impose au juge de faire reposer sa décision de culpabilité ou d'innocence uniquement sur les éléments de preuve issus de la procédure pénale. En outre, le contradictoire implique que toutes les pièces produites par l'une des parties soient communiquées à l'autre[1254] et peuvent être admises durant l'audience[1255]. Il exige que toutes les preuves inscrites dans le dossier de la procédure soient soumises à la libre discussion des parties lors des débats.

475. L'association de technologies algorithmiques en vue d'analyser les images collectées aux drones aériens de sécurité publique devrait venir modifier les conditions d'admissibilité de la preuve. En ce sens, ces algorithmes d'analyse d'images à des fins d'aide à la prise de décision sont susceptibles de questionner le respect effectif par les forces de l'ordre des principes inhérents à la procédure pénale dans la mesure où ils font encore preuve d'une insuffisante fiabilité et d'une certaine forme d'opacité de leur fonctionnement.

[1250] SONTAG-KOENIG (S.), « Sonorisation et fixation d'images : que reste-t-il de la vie privée ? », *AJP* n° 1, 30 janvier 2023, p. 27. Voir aussi : GUÉRIN (D.), « La loyauté de la preuve devant le juge pénal », *Procédures* n° 4, 2015, Dossier 11.

[1251] Conv. EDH, art. 8 ; DDHC, art. 2 ; CP, art. 226-1 ; CEDH, 29 mars 2005, *Matheron c. France*, n° 57752/00, §29 [en ligne].

[1252] SUDRE (F.), *Droit européen et international des droits de l'homme*, Paris, PUF, 15ème édition, 2021, 1044 p., n° 150 et suiv. ; SONTAG-KOENIG (S.), « Sonorisation et fixation d'images : que reste-t-il de la vie privée ? », *op. cit.*

[1253] CPP, article préliminaire §1 : « la procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties ».

[1254] C. cass., ch. crim., 17 décembre 1970, n° 68-91.412 [en ligne].

[1255] C. cass., ch. crim., 3 octobre 2012, n° 11-88.468 [en ligne].

B. Les limites à l'admissibilité de la preuve pénale issue des drones aériens « augmentés » de sécurité publique

476. Les technologies ont largement contribué à l'établissement de la preuve dans le cadre du procès pénal et sont souvent privilégiées par les forces de l'ordre[1256]. Néanmoins, le principe de licéité de la preuve impose que les éléments obtenus au travers de ces technologies respectent les principes inhérents au procès pénal. Dès lors, ces principes devront également s'appliquer aux drones aériens « augmentés » de sécurité publique. Au sein des principes qui régissent le procès pénal, la présomption d'innocence constitue un pilier du droit à la sûreté en ce qu'elle permet de lutter contre les décisions qui mèneraient à des arrestations et détentions arbitraires. Or, ce principe pourrait être bousculé par l'introduction des algorithmes d'analyse d'images couplés aux caméras de vidéoprotection dans la mesure où les résultats qu'ils produisent peuvent être faussés par des biais ou des erreurs susceptibles d'influencer les forces de l'ordre dans leur prise de décisions (1). Aussi, le recours à ces technologies, au regard du contexte d'opacité auquel elles sont encore sujettes ne permet pas de garantir le respect des principes qui régissent la procédure pénale (2).

1. Les drones aériens « augmentés » de sécurité publique facteurs de potentielles atteintes à la présomption d'innocence

477. Les analyses issues du chapitre précédent ont permis d'établir le fait que les algorithmes « augmentés » ne sont pas infaillibles. Dès lors, l'analyse des images issues des drones aériens « augmentés » de sécurité publique est susceptible de produire des résultats erronés ou biaisés[1257] et ce en dépit des efforts menés par leurs concepteurs. En conséquence, ces technologies pourraient induire en erreur les agents des forces de l'ordre dont les décisions reposeront pour part sur les résultats produits par l'algorithme. Or, ces erreurs décisionnelles, mettant en accusation un individu, auraient pour effet de conduire à des arrestations voire à des détentions arbitraires. En ce sens, les algorithmes d'analyse d'images issues des drones aériens de sécurité publique porteraient atteinte à l'essence même du droit à la sûreté. Aussi, la suppression du droit de ne pas pouvoir faire l'objet de

[1256] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 100.

[1257] Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 150 : « aussi sophistiqués qu'ils puissent être, ces systèmes restent faillibles : ils peuvent se tromper et mal classifier les individus qu'ils évaluent avec, comme conséquence, des effets potentiellement désastreux sur leur vie » ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit*., p. 56 : « Il faut prendre conscience que les SAAD ne sont pas infaillibles, dans le sens où ils peuvent réaliser des prédictions erronées conduisant à de mauvaises décisions ».

soupçons, autrefois inscrit dans le droit à la sûreté de la DDHC[1258], a très largement participé à atténuer la garantie du principe de la présomption d'innocence.

478. Le recours à des algorithmes d'analyse d'évènements à des fins de détection d'individus susceptibles de commettre une infraction pourrait réduire l'effectivité du principe de la présomption d'innocence - pourtant inhérent au procès pénal - qui subsisterait davantage de manière théorique qu'en pratique. Pourtant, la présomption d'innocence est un principe essentiel en matière pénale dans la mesure où elle sert à protéger la personne poursuivie « contre les jugements de valeur sur sa culpabilité »[1259]. En outre, elle s'impose à l'État au travers de ses représentants[1260]. Cependant, les nouvelles technologies auraient notamment tendance à amplifier les atteintes portées à ce principe[1261]. Dès lors, cette garantie procédurale pourrait être remise en question par les drones aériens « augmentés » de sécurité publique.

479. Un problème se pose plus particulièrement lorsqu'un élément de preuve numérique se voit automatiquement conférer le statut de preuve irréfutable au motif que la technologie serait plus fiable qu'un être humain. En ce sens, la magistrate Hélène Cazaux-Charles s'inquiétait de la possibilité que le résultat (donc une probabilité) d'un algorithme « ne devienne une certitude et qu'un soupçon ne devienne une preuve »[1262]. L'enjeu avait déjà été soulevé, lorsqu'avaient été introduites les premières caméras de surveillance, d'être tenté de considérer les images obtenues par ces systèmes comme nécessairement irréfutables. L'introduction des caméras « augmentées » pourrait venir aggraver cette propension à vouloir se reposer sur les résultats de l'algorithme comme étant une preuve irréfutable, ce qui contreviendrait au respect tant du principe de présomption d'innocence qu'au principe du contradictoire. Une telle situation témoignerait alors de l'effritement de l'État de droit. En outre, l'existence de biais et d'erreurs algorithmiques démontrent que les

---

[1258] DDHC, art. 7 : « Nul homme ne peut être accusé, arrêté ou détenu que dans les cas déterminés par la loi […] ».

[1259] ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 178.

[1260] VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 58. Voir en ce sens : CEDH, 10 février 1995, *Allenet de Ribemont c. France*, n° 15175/89 [en ligne].

[1261] Les médias numériques, allant de la presse publique aux vidéos postées sur internet, tendent à favoriser les atteintes portées à la présomption d'innocence. Voir en ce sens : Ministère de la Justice, Rapport sur « La présomption d'innocence : un défi pour l'Etat de droit » remis par GUIGOU (É.), octobre 2021, 217 p., p. 19 [en ligne] : « Les atteintes au principe de la présomption d'innocence émanent de l'ensemble des acteurs de la société : les acteurs institutionnels, les médias, mais aussi, du fait de la place prise en quelques années par les réseaux sociaux, un nombre considérable de personnes ».

[1262] Propos de Hélène Cazaux-Charles dans : LE NEVÉ (S.), « La justice prépare sa révolution algorithmique », *Acteurs Publics*, 27 juin 2017 [en ligne] consulté le 4 juillet 2019.

résultats ne peuvent être reconnus comme irréfutables.

480. Aussi, la recherche de potentiels auteurs d'infractions au moyen de drones aériens « augmentés » de sécurité publique pourrait être assimilée à la recherche de personnes « dangereuses » dans la mesure où ils ne se contentent pas de constater les infractions mais sont à la recherche de la commission d'une infraction[1263]. Dès lors, cette volonté de vouloir assurer la protection des personnes par une anticipation des agissements d'individus pouvant être reconnus comme « dangereux » au sens que lui donnerait l'algorithme d'analyse d'évènement ne serait pas sans conséquences sur les droits et libertés. Cette recherche de personnes « dangereuses » n'est pas sans rappeler la notion de « dangerosité criminologique » inscrite dans le droit pénal lors du renforcement des mesures de sûreté[1264]. Ces mesures à caractère individuel et coercitif sont « imposées à des individus qualifiés de dangereux pour l'ordre social afin de prévenir les infractions que leur état rend probable »[1265]. Plusieurs auteurs ont depuis longtemps manifesté leur inquiétude à l'égard du concept de dangerosité[1266]. De fait, l'apparition du terme de « dangerosité » ne tend pas uniquement à déshumaniser le droit pénal mais engendre une redéfinition de son essence en se substituant au terme de « culpabilité ». Dès lors, la « dangerosité » permet de privilégier les mesures de précaution (mesures de sûreté) sur la peine. En outre, le terme de « dangerosité » fait place à une

---

[1263] BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 13 : L'emploi de drones aériens de sécurité publique à des fins préventives servira « surtout pour rechercher coercitivement la commission d'infractions dans le cadre d'une activité de police administrative ».

[1264] Voir en ce sens : CPP, art. 723-29 à 723-39 et R. 61-7 à R. 61-11.

[1265] BOULOC (B.), *Droit pénal général,* Paris, Dalloz, coll. Précis droit privé, 23ème édition, 2013, 950 p., pp. 427 et suiv.

[1266] DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 43 ; BASEX (H.), MBANZOULOU (P.) ET RAZAC (O.), « Introduction » *in* BASEX (H.), MBANZOULOU (P.), RAZAC (O.) et ALVAREZ (J.) (dir.), *Les nouvelles figures de la dangerosité*, Paris, L'Harmattan, 2008, 402 p., pp. 15-19 ; ALIX (J.), « Une liaison dangereuse. Dangerosité et droit pénal en France » *in* GIUDICELLI-DELAGE (G.) et LAZERGES (C.) (dir.), *La dangerosité saisie par le droit pénal*, Paris PUF, IRJS éditions, coll. Les voies du droit, 2011, 320 p., pp. 49-78 ; DELMAS-MARTY (M.), « Sécurité et dangerosité », *RFDA* n°6, 10 janvier 2012, p.1096 ; LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *RSC* n° 3, 23 novembre 2018, p. 573 : « S'il existe un concept de dangerosité, il appartient à la catégorie des concepts insaisissables, mouvants, sans frontières et ce, alors même que les algorithmes prédictifs connaissent un essor sans précédent. La dangerosité du concept de dangerosité n'est plus à démontrer, il se construit depuis la nuit des temps sur la peur, les peurs et le mirage du risque zéro ».

incompréhension terminologique[1267] accentuée par une absence de définition unanime[1268].

481. Pourtant, la loi pénale repose sur la recherche de la vérité et désigne le juge comme seul compétent dans cette détermination. Cependant, face au climat de peur qui s'est installé ces vingt dernières années, le droit pénal fait l'objet d'importantes mutations en basculant progressivement non plus vers une recherche de la culpabilité de la personne poursuivie mais vers celle de sa dangerosité. Cette recherche aura conduit au développement et au recours de plus en plus fréquent d'une science criminologique soutenant être en mesure d'établir « un diagnostic de dangerosité et un pronostic de récidive » reléguant le juge au rang de « simple chambre d'enregistrement »[1269].

482. Les drones aériens « augmentés » de sécurité publique pourraient avoir pour finalité de déterminer, sur la base d'une évaluation des gestes voire de la démarche, la dangerosité d'un individu. Dès lors, il s'agirait pour un algorithme d'outrepasser une évaluation humaine dans le processus d'évaluation de la dangerosité d'un individu. Le pouvoir décisionnel du juge serait alors en partie soumis aux conditions des algorithmes (qui « agiraient » à l'instar des criminologues). La justice s'en trouverait alors autant déshumanisée (en reposant partiellement sur une machine) que déjudiciarisée dans la mesure où la vidéo serait reconnue comme établissant des faits admissibles comme preuve *a priori* irréfutable associée à des résultats de l'algorithme *a priori* incontestables[1270]. La garantie que confère la liberté individuelle serait par conséquent sérieusement obérée.

[1267] Voir notamment : DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 22 ; MBANZOULOU (P.), « La dangerosité des détenus. Un concept flou aux conséquences bien visible : le PSEM et la rétention de sûreté » *in* BASEX (H.), MBANZOULOU (P.), RAZAC (O.) et ALVAREZ (J.) (dir.), *Les nouvelles figures de la dangerosité*, *op. cit.*, p. 171 ; LAZERGES (C.), « Le choix de la fuite en avant au nom de la dangerosité », *RSC*, janvier/mars 2012, pp. 274-283.

[1268] ALIX (J.), « Une liaison dangereuse. Dangerosité et droit pénal en France » *in* GIUDICELLI-DELAGE (G.) et LAZERGES (C.) (dir.), *La dangerosité saisie par le droit pénal*, *op. cit.*, p. 76.

[1269] DELMAS-MARTY (M.), « Sécurité et dangerosité », *op. cit.*

[1270] Un tel scénario remettrait également en question la séparation entre le pouvoir judiciaire et le pouvoir exécutif où ces technologies deviendraient un moyen de détourner le pouvoir judiciaire en le vidant progressivement de sa substance entrainant un processus de déstructuration de l'État de droit.

2. L’opacité des drones aériens « augmentés » de sécurité publique porteuse d’atteintes aux droits de la procédure pénale

483. Les analyses précédentes ont démontré que les technologies « augmentées » pâtissent encore d’une importante opacité de leur fonctionnement. Dès lors, les caméras « augmentées » de sécurité publique seront aussi susceptibles de présenter des défauts en matière de transparence et d’explicabilité de leurs algorithmes. Or, l’absence de transparence et d’explicabilité peut engendrer de potentielles atteintes aux droits de la défense dans la mesure où elle contreviendrait au droit au procès équitable[1271]. Ce droit comprend plusieurs principes qui s’appliquent à la procédure pénale[1272] incluant la présomption d'innocence, l’égalité des parties devant le juge et le principe du contradictoire.

484. Le droit au procès équitable suppose que « l’accusé doit pouvoir participer "réellement" à son procès »[1273] en application des principes de l’« égalité des armes » entre les parties et du contradictoire. Dès lors, l’absence de compréhension du fonctionnement voire de connaissance du traitement par les algorithmes « augmentés » associés à des drones aériens de sécurité publique méconnaitrait ce droit en introduisant un déséquilibre entre les détenteurs de la puissance publique et la personne poursuivie. Cette opacité porterait atteinte au principe du contradictoire dans la mesure où la personne inculpée ne serait pas en mesure de questionner la pertinence des résultats fournis par l’algorithme.

485. Aussi, le caractère dématérialisé des SIA d’analyse d'images de vidéoprotection engendre des difficultés quant à la mise en œuvre de l’information du traitement de DACP à des fins pénales auprès des personnes concernées pouvant faire l’objet d’une arrestation. Or, l’opacité de ces technologies pourrait porter atteinte à l’exercice des droits de la défense de la personne faisant l’objet d’une arrestation voire d’une détention[1274]. Dès lors, les principes de transparence et d’explicabilité des algorithmes constituent des éléments essentiels tant à la conception qu’à

[1271] Conv.EDH, art. 6.

[1272] ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 39.

[1273] SUDRE (F.), *La convention européenne des droits de l’Homme*, *op. cit.*, p. 98.

[1274] CHEMI, Rapport final sur l’« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBES (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 40.

l'utilisation de ces technologies « augmentées » de sécurité publique qui participent au maintien des droits de la défense.

§2. L'incidence sur l'État de droit du recours à des drones aériens « augmentés » de sécurité publique

486. En dépit des nombreuses garanties des droits et libertés érigées au cours des siècles, il est à déplorer que face aux menaces pesant sur l'ordre public le droit français « s'accommode de régressions, de textes d'exception ou de zones d'ombre inacceptables »[1275]. En tentant de répondre à la demande grandissante en faveur d'une amélioration de la sécurité des personnes et des biens, le législateur n'a eu de cesse d'adopter des dispositions toujours plus restrictives des droits et libertés[1276], à l'instar des lois en matière de lutte contre le terrorisme. Ces « zones d'ombre » pourraient se traduire par le caractère souvent inadapté de la législation, plus particulièrement s'agissant des usages technologiques. En ce sens, les drones aériens de sécurité publique ont longtemps pâti non pas d'un vide juridique mais d'une inadéquation d'encadrement pour faire face aux nouveaux enjeux engendrés. En outre, ces « zones d'ombre » pourraient faire référence à l'insuffisance de clarté dans les moyens effectivement mis en œuvre pour garantir les droits et libertés telle qu'en matière de recours à des technologies de surveillance à des fins de sécurité publique. Il en va ainsi de la loi RPSI et de son décret d'application, dont les dispositions n'apportent aucune précision s'agissant des moyens concrets pour respecter l'obligation d'information du public lors du recours à des drones aériens de sécurité publique.

487. Face aux exigences de l'ordre public, l'État a pris de longue date la décision de recourir à des outils technologiques aux fins d'assurer la sécurité publique[1277]. Les technologies « augmentées » se présentent comme des solutions prometteuses et pourraient notamment améliorer l'efficacité des forces de l'ordre dans l'exercice de leurs missions[1278] - sous réserve d'être utilisées

---

[1275] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 14.

[1276] Voir en ce sens l'annexe 3 sur les lois en matière de sécurité publique et de sécurité intérieure qui octroient de nombreuses prérogatives aux forces de l'ordre à des fins préventives comme répressives.

[1277] Pour rappel, la LOPS, adoptée en 1995, a permis d'autoriser l'installation de caméras fixes filmant la voie publique (v. n° **95**).

[1278] DANAHER (J.), "The threat of Algocraty : Reality, Resistance and Accommodation", *Philosophy & Technology*, vol. 29 (3), 2016, pp. 245-268. Voir aussi : Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 23 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 6.

de manière responsable[1279]. Néanmoins, le choix politique de mettre en œuvre des drones aériens « augmentés » de sécurité publique n'est pas neutre dans la mesure où ils permettent d'accroitre les possibilités de surveillance[1280] et potentiellement remettre en question une part de l'autonomie des agents des forces de l'ordre dans leur prise de décisions[1281] (A). En outre, le recours systématique aux nouvelles technologies et l'introduction de technologies de surveillance « augmentées » de sécurité publique participe d'une pérennisation de règles d'exception qui restreignent l'exercice des droits et libertés mettant en péril l'État de droit (B).

A. L'enracinement d'un régime de suspicion par le recours aux drones aériens « augmentés » de sécurité publique

488. L'introduction du concept de « sécurité » a permis d'ouvrir un nouveau champ de recherches dans différents domaines dont celui des technologies à des fins de surveillance. L'arrivée de la surveillance et, par voie de conséquence, le contrôle de la population a propulsé le concept de sécurité au premier plan des sujets de la politique de l'État français. La place prépondérante qu'occupe actuellement ce concept de « sécurité » permet d'amorcer un « tournant sécuritaire » au sein duquel s'inscrit la surveillance. Ce tournant fait apparaitre un double enjeu de l'identification des individus, d'une part, et de la gestion des circulations sur des territoires, d'autre part[1282].

489. Le concept de « sécurité » se concentre sur les individus dans leur ensemble, en d'autres termes sur les personnes perçues de manière collective. Cette vision du collectif tend à renforcer les mesures établies dans le cadre de l'intérêt général. Toutefois, celle-ci ne doit pas, pour autant, conduire à une atteinte disproportionnée voire à la disparition des libertés individuelles. En outre, la vision collectiviste associée aux outils technologiques de surveillance présente le risque de déshumaniser la population. En ce sens, elle serait alors réduite à « un ensemble de processus physiques « naturels » sur lesquels on peut agir de toutes les manières possibles (lois et règlements,

---

[1279] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 14.

[1280] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 15.

[1281] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, op. cit., p. 53 : « on peut penser que, dans un contexte de décisions routinière, la vigilance de l'humain qui prend une décision est amoindri et que, de fait, c'est la machine qui prend la décision » ; LELIEUR (J.), « L'intelligence artificielle : une nouvelle technologie probatoire en émergence », *op. cit.*

[1282] AÏM (O.), *Les Théories de la surveillance : Du panoptique aux Surveillance Studies*, Malakoff, Armand Colin, 2020, 253 p., p. 97.

bien sûr, mais aussi habitudes, modes de vies, actions sur le milieu, salubrité, fluidité des circulations, etc.). Bref, gouverner une population, c'est agir sur toutes les variables qui guident son comportement général »[1283].

490. La concentration des efforts orientée sur les individus en tant que simples données ou informations biologiques altère la manière de gouverner. L'État se veut être en mesure de pouvoir agir face à tout type d'évènement tel que le décrit Michel Foucault : « Il va falloir manipuler, il va falloir susciter, il va falloir faciliter, il va falloir laisser faire, il va falloir, autrement dit, gérer et non plus réglementer »[1284]. En d'autres termes, le philosophe affirme que la sécurité entrainerait une nouvelle forme d'encadrement par l'État non par l'intermédiaire de la réglementation mais par celle de la régulation[1285]. Or, les dernières technologies « augmentées » développées à des fins d'analyse d'images de la voie publique vont en ce sens. Certains auteurs, tels le magistrat Yannick Meneceur, dénoncent ainsi le recours à des SIA dans la police comme étant des « dérives solutionnistes »[1286]. Dès lors, les drones aériens « augmentés » de sécurité publique interrogent quant à la proportionnalité de leur usage par les forces de l'ordre dans le respect des droits et libertés garantis et leur incidence sur l'État de droit.

B. L'incidence du recours à des drones aériens « augmentés » de sécurité publique sur l'État de droit

491. Les attentats qui se sont déroulés dans le monde depuis le 11 septembre 2001 ont eu pour effets indirects de permettre en de nombreuses occasions aux dirigeants politiques de passer outre l'obligation de respecter les limites qu'impose l'État de droit tant de manière symbolique qu'au plan juridique[1287]. Or, l'État de droit impose que « tous les pouvoirs publics agissent dans les limites

---

[1283] RAZAC (O.), *Après Foucault, avec Foucault : Disséquer la société de contrôle*, Paris, L'Harmattan, 2008, p. 38.

[1284] FOUCAULT (M.), *Sécurité, territoire, population*, Cours au Collège de France 1977-1978, Paris, Le Seuil, 2004, p. 360.

[1285] Le terme de « régulation » est utilisé de manière récurrente s'agissant de l'encadrement de la conception et de l'usage des algorithmes d'IA à l'instar de Thierry Breton (commissaire européen) qui en évoquant le vote par le Parlement européen du texte sur l'IA énonçait que « c'est bien la régulation qui donne la sécurité juridique nécessaire aux start-ups pour l'innovation » (« Pour Thierry Breton, la régulation des IA est analogue au permis de conduire », *NextInpact*, 20 juin 2023 [en ligne]). Voir aussi de manière non-exhaustive :« Le Parlement européen adopte un projet de loi pour réguler l'intelligence artificielle », *rfi.fr*, 14 juin 2023 [en ligne] ; « L'intelligence artificielle : ne pas se tromper de régulation », *lemonde.fr*, 10 juin 2023 [en ligne]. Il s'agit pourtant d'une erreur probablement (une nouvelle fois) dérivée d'une traduction du terme anglo-saxon *regulation* qui signifie en réalité « réglementation ».

[1286] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 94.

[1287] DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 9.

fixées par la loi, conformément aux principes de la démocratie et des droits de l'homme, et sous le contrôle de tribunaux indépendants et impartiaux »[1288]. En d'autres termes, il désigne « un État soumis au droit impliquant les garanties juridiques institutionnelles (séparation des pouvoirs) et substantielles (respect des droits fondamentaux) »[1289]. Cependant, les drones aériens « augmentés » de sécurité publique, compte tenu des enjeux qu'ils engendrent encore, pourraient porter atteinte à l'État de droit. En ce sens, ces technologies ne sont pas encore en mesure d'assurer de manière effective le respect de principes tels la transparence, l'égalité et la non-discrimination ou encore la protection du droit au procès équitable pourtant imposés par l'État de droit[1290].

492. Face aux réels dangers que présente l'accroissement de la criminalité et du terrorisme, les responsables politiques peuvent avoir recours à des solutions exceptionnelles qui portent atteinte aux droits et libertés. En d'autres termes, il s'agit de mettre en œuvre des règles d'exception pour faire face à des évènements à caractère exceptionnel, tel qu'une attaque terroriste, sous condition et de manière limitée dans le temps. Or, il a déjà été observé que de telles règles d'exception fassent l'objet d'une pérennisation[1291]. Pourtant, un tel acte n'est pas anodin dans la mesure où la pérennisation de règles d'exception tend à légitimer des pratiques contraires à l'État de droit telle que la déshumanisation du droit pénal introduisant notamment la notion de dangerosité, le durcissement des procédures de contrôle par l'État ou encore l'installation pernicieuse de régimes de suspicion[1292]. Il existe par conséquent un réel risque de porter atteinte aux droits et libertés lorsqu'ils ne sont pas garantis de manière effective, au motif de vouloir assurer la défense de l'État[1293]. En outre, Michel Troper faisait remarquer que le fait d'inclure les « actes terroristes » à la liste des circonstances exceptionnelles introduit un doute quant au caractère provisoire des mesures mises en œuvre dans la mesure où il parait difficile d'imaginer "un moment où cesserait toute

---

[1288] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 14.

[1289] DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », *op. cit.*, p. 467.

[1290] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 14.

[1291] Voir en ce sens : Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *op. cit.*, qui avait permis de pérenniser la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *op. cit.* ; SAFI (F.), « La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement : Entre pérennisation et extension de l'exception… », *op. cit.*

[1292] BIGO (D.) *et al.* (dir.), *Suspicion et exception*, Paris, L'Harmattan, 2008, 222 p.

[1293] DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », *op. cit.*, p. 467.

menace de terrorisme »[1294]. Dès lors, en introduisant la « prévention d'actes de terrorisme » parmi les finalités d'utilisation des drones aériens de sécurité publique, le législateur laisse apparaitre un doute s'agissant des limites temporelles imposées à l'usage de cette technologie par les forces de l'ordre qui pourrait porter une atteinte disproportionnée aux droits et libertés.

493. L'intégration progressive de technologies de surveillance « augmentées » au sein des outils à l'usage des forces de l'ordre suscite légitimement l'inquiétude des défenseurs des droits et libertés qui y voient une forme de surveillance de masse par l'État. Les premiers concernés reconnaissent cependant la nécessité « de disposer d'outils d'analyse décisionnels en phase avec les exigences d'une société démocratique connectée, qui fait rimer transparence et égalité, avec une forte attente de prévisibilité des risques et de la capacité à anticiper pour les annihiler »[1295]. Néanmoins, il apparait que le fait de vouloir anticiper tout évènement susceptible d'engendrer une atteinte à la sécurité des personnes, de leurs biens ou des institutions de l'État au moyen de technologies de surveillance « augmentées » participe au mouvement de pérennisation d'un état d'exception. En ce sens, ces technologies entreraient dans le « mythe d'une sécurité totale » qui « se fonde sur l'illusion qu'il serait possible de prévoir le futur avec certitude et de le contrôler par anticipation »[1296]. Ce mythe serait alors incompatible avec l'État de droit dans la mesure où il ne serait alors plus soumis aux limites imposées par le droit[1297]. Aussi, le recours massif aux outils de surveillance, aujourd'hui souvent associés à des SIA, ne fait qu'amplifier le phénomène de suspicion généralisée de chaque individu.

494. Enfin, indépendamment des enjeux que suscite l'emploi de technologies « augmentées » à des fins de sécurité publique, l'impunité dont bénéficient les forces de l'ordre quant à l'usage de nouvelles technologies en dehors de tout cadre réglementaire adapté remet en question l'effectivité des garanties existantes des droits et des libertés face à une surveillance toujours plus étendue et

---

[1294] TROPER (M.), « L'État d'exception n'a rien d'exceptionnel » *in* THÉODOROU (S.) (dir.), *L'État d'exception dans tous ses états*, Marseille, Éditions Parenthèses, 2007, 294 p., pp. 163-176, p. 163.

[1295] LAGASSE (J.), « Algorithmes et politiques publiques de sécurité, quels nouveaux paradigmes ? », *Revue de la Gendarmerie nationale*, 2nd Semestre 2018, pp. 47- 54, spéc. p. 47.

[1296] CAMUS (C.), *La Guerre contre le terrorisme. Dérives sécuritaires et dilemme démocratique*, Paris, Éditions Le Félin, 2007, 151 p., p. 137. Voir aussi : DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », *op. cit.*, p. 470 : « La "frénésie sécuritaire" tend à transformer le contrat social en une sorte de contrat d'assurance tous risques qui caractérise les régimes de suspicion : chaque individu est un suspect potentiel. […] Aussi, les régimes de suspicion entrainent-ils inévitablement un détournement de l'État de droit ».

[1297] CAMUS (C.), *La Guerre contre le terrorisme. Dérives sécuritaires et dilemme démocratique*, *op. cit.*, p. 137

intrusive de la voie publique[1298]. Si la réponse aux exigences de l'ordre public par des moyens technologiques est légitime, elle ne doit pas contraindre le droit. À l'inverse, le législateur doit anticiper les évolutions technologiques et repenser le processus de conception des lois en faisant appel à tous les acteurs concernés notamment aux citoyens[1299], en vue de garantir le respect effectif des droits et libertés.

[1298] De manière similaire, la professeure Mireille Delmas-Marty avait remarqué que le « contournement des droits substantiels s'accompagn[ait] parfois de celui des institutions compétentes […] comme la Commission nationale de l'informatique et des libertés (CNIL) » (DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », *op. cit.*, p. 474).

[1299] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 52-53 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 205-206.

CONCLUSION DU TITRE II

495. Les drones aériens « augmentés » de sécurité publique modifient la nature et l'incidence de la surveillance de la voie publique sur les personnes concernées. La mise en œuvre du cadre juridique autorisant le recours à des drones aériens par les forces de l'ordre se révèle insuffisant pour garantir une protection effective des droits et libertés face à l'arrivée des algorithmes d'analyse d'images auxquels ils seront associés. Indépendamment de l'incidence sur le comportement et des potentielles atteintes aux droits des personnes surveillées, les drones aériens « augmentés » de sécurité publique tendent à amplifier les enjeux relatifs à la sécurité des données collectées dont les conséquences pourraient être d'affecter le déroulement de la procédure pénale. En outre, l'introduction des technologies de surveillance « augmentées » s'inscrit dans la continuité d'une coproduction de sécurité entre autorités publiques et entités privées dont les effets sont autant porteurs de bénéfices que de contraintes. Ces technologies d'aide à la prise de décisions par les agents des forces de l'ordre sont ainsi susceptibles d'améliorer l'exercice de leur activité mais pourraient laisser planer le doute quant au respect du principe interdisant la délégation de pouvoirs de police à des personnes privées.

496. Aussi, l'opacité et l'insuffisance de fiabilité des technologies « augmentées » ne permettent pas aux drones aériens « augmentés » de sécurité publique d'être en mesure d'assurer le respect des principes inhérents au procès pénal dont le droit au procès équitable permet notamment de prévenir les atteintes portées à la présomption d'innocence. Or, ces principes sont au cœur des fondements de l'État de droit. Dès lors, ces technologies seraient susceptibles d'engendrer une forme de mutation de l'État de droit en pérennisant des règles d'exception qui restreignent de manière disproportionnée les droits et libertés. Le recours à des drones aériens « augmentés » de sécurité publique nécessite par conséquent la prise en compte effective des enjeux liés à leur conception et à leur usage dans un souci de rééquilibrer le rapport entre autorités publiques et administrés ainsi que d'assurer la protection effective des droits et libertés.

CONCLUSION DE LA PREMIÈRE PARTIE

497. Les potentialités que présentent les technologies de surveillance d'améliorer l'exécution des missions de sécurité publique n'ont pas échappé aux forces de l'ordre dans leur quête de réponses aux exigences de l'ordre public. Face à la demande émanant des services de sécurité publique, d'une part, et des citoyens, d'autre part, le législateur a œuvré en faveur d'une introduction progressive des caméras de surveillance sur la voie publique.

498. Néanmoins, le souci d'adapter la réponse législative aux besoins des forces de sécurité publique, d'une part, et aux évolutions technologiques croissantes, d'autre part, a renforcé les restrictions portées à l'exercice des droits et libertés. L'introduction des drones aériens de sécurité publique constituait déjà un renforcement de la surveillance de la voie publique par le caractère intrusif dû à leur mobilité et leur discrétion limitant la protection du droit à la vie privée et des DACP. Aussi, l'association de ces technologies à des SIA, compte tenu de leurs écueils subsistants, est susceptible d'engendrer des atteintes à la liberté individuelle et de manière plus étendue à l'État de droit. Le rapport sûreté-sécurité semble ainsi pâtir de l'introduction des drones aériens « augmentés » de sécurité publique en favorisant excessivement la sécurité au détriment de la sûreté.

499. Le cadre régissant le rapport sûreté-sécurité a subi de nombreux remaniements depuis la DDHC et nécessitera un renouvellement en vue de résoudre les enjeux auxquels font face les drones aériens « augmentés » de sécurité publique. Le recours à cette technologie pourrait être effectué dans un cadre respectueux des droits et libertés par la mise en œuvre de mesures générales et spécifiques, d'ordre juridique et technique, et en mobilisant tous les acteurs impliqués.

Deuxième partie

UNE NÉCESSAIRE REDÉFINITION DU RAPPORT SÛRETÉ-SÉCURITÉ INDUITE PAR LES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

500. Les drones aériens « augmentés » de sécurité publique soulèvent une question bien connue du droit énoncée par Montesquieu dans *De l'esprit des lois* à savoir « comment concilier la sûreté de l'État avec la sûreté de la personne ? »[1300]. Il faut comprendre le sens de cette question comme une référence faite à la nécessaire conciliation entre les besoins de la collectivité et la préservation des droits et libertés de la personne (besoins individuels). Montesquieu reprend ainsi le fondement de la relation qui lie la sûreté et l'ordre public. Pourtant, ce que le philosophe mentionne sous les termes de « sûreté de l'État » serait désormais désigné sous le terme de « sécurité », et les termes de « sûreté de la personne » correspondent aujourd'hui aux « libertés individuelles » composées de la « liberté individuelle » et de la « liberté personnelle » (**Titre 1**).

501. Face aux enjeux que posent les technologies de surveillance de la voie publique, les instances nationales et européennes tentent d'élaborer un encadrement adapté à leurs évolutions afin de renforcer et d'introduire des garanties dans l'espoir d'offrir une protection concrète des droits et libertés. Les usages des technologies de surveillance « augmentées » par les SAAD nécessitent une nouvelle approche juridique permettant d'assurer le fonctionnement de ces outils autant qu'une conception et un usage respectueux des droits et libertés (**Titre 2**).

[1300] MONTESQUIEU (C.), *L'esprit des lois*, 1748, Livre V, chap. XIV.

TITRE I L'AFFAIBLISSEMENT DE LA PROTECTION DE LA SÛRETÉ, GARANTE DES DROITS ET LIBERTÉS, À L'ÈRE DES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

502. Malmenée mais non détruite, la sûreté se voulait être, pour les rédacteurs de la DDHC, la mesure permettant d'assurer l'équilibre entre les libertés et l'ordre public[1301]. Néanmoins, elle n'est pas exempte de restrictions lorsque des circonstances exceptionnelles l'exigent. Afin de prévenir les dérives que ces limites peuvent porter à l'ensemble des droits et libertés, plusieurs dispositifs juridiques ont été progressivement mis en œuvre en vue de préserver son exercice et d'encadrer ces restrictions de manière stricte.

503. En premier lieu, les sources normatives, nationales et supranationales, sont une première forme de protection des droits et libertés. Certaines énoncent de manière claire la notion de sûreté en tant que liberté propre à chaque individu face aux décisions arbitraires d'un État. D'autres y font référence usant d'une autre terminologie telle que la liberté individuelle. Toutefois, ces sources trouvent leurs limites à mesure que se multiplient les politiques publiques en faveur d'une plus grande sécurité des États et de leur population au point de substituer à la notion de sûreté un concept de sécurité que le législateur tente d'ériger en droit fondamental (**Chapitre 1**).

504. En deuxième lieu, différents acteurs sont chargés de garantir la protection des droits et libertés. Ces dernières années, l'inflation normative et l'insistance pour une politique plus sécuritaire ont contribué à limiter la protection concrète des droits et libertés qu'assurent ces garants. Aussi, l'introduction des technologies de surveillance à des fins de sécurité publique a sensiblement modifié l'importance des pouvoirs des différents acteurs, juridictionnels comme non-juridictionnels, dans leur rôle de garants des droits et libertés (**Chapitre 2**).

[1301] FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 204 : « Le droit à la sûreté pose le principe d'une garantie générale contre toute forme d'arbitraire […] Aussi, il importait pour les révolutionnaires de 1789 d'inscrire dans une déclaration des droits celui qui devait conditionner la pleine jouissance de tous les autres, en garantissant au citoyen que le pouvoir de l'État ne s'exercerait plus sur lui de façon arbitraire et excessive » ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 315 : « Le respect de la sûreté personnelle […] exige une nécessaire conciliation entre la garantie de la liberté individuelle et l'indispensable répression étatique, dans une société, de tout comportement contraire aux autres libertés individuelles ».

CHAPITRE 1 L'ÉVOLUTION DU RAPPORT SÛRETÉ-SÉCURITÉ À L'ÈRE DES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

505. Saisir le sens du rapport entre sûreté et sécurité nécessite de revenir aux origines des textes fondateurs des droits et libertés. En France, les droits et libertés ont été « codifiés » au sein de la DDHC du 26 août 1789, reconnue comme l'un des premiers textes suprêmes du droit français. Encore aujourd'hui, le Conseil constitutionnel se fonde sur les articles de la DDHC afin de mettre en lumière des notions cardinales sur lesquelles repose le droit français et ériger des droits et libertés au rang suprême de droits et libertés fondamentaux[1302]. L'appréhension de l'évolution du rapport entre sûreté et sécurité nécessite d'étudier les fondements de la notion de sûreté et de son évolution afin de mieux discerner les raisons qui ont conduit à l'apparition du concept de sécurité (**Section 1**).

506. L'étude de l'évolution législative et jurisprudentielle entourant le rapport entre sûreté et sécurité permettra d'aborder un débat qui anime fortement la doctrine ces dernières années concernant l'existence d'un droit à la sécurité et de sa potentielle fondamentalisation. En outre, l'apparition de nouvelles technologies de surveillance de sécurité publique tend à amplifier un phénomène d'atténuation de la frontière distinguant les activités de police judiciaire de celles relevant de la police administrative (**Section 2**).

Section 1 Le bouleversement progressif du rapport sûreté-sécurité à l'ère des technologies de surveillance de la voie publique

507. Étudier l' « esprit » originel du texte de la DDHC semble incohérent au vu du caractère matériel de celui-ci. Pour autant, cet angle d'approche n'est pas dénué d'utilité lorsque le terme d'« esprit » associé aux droits de l'Homme fait référence au sens qu'en donnait Montesquieu dans son *Esprit des lois*[1303]. Tel que l'entendait le philosophe, le terme d' « esprit » s'assimile à l'intention ou encore à la direction que souhaitaient donner les auteurs au contenu de la DDHC et

---

[1302] À titre d'exemple : Le droit au respect de la vie privée est rattaché à l'article 2 de la DDHC (C. const., Décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, Rec. p. 100, cons. 45 [en ligne]) ; la liberté d'aller et venir est rattachée aux articles 2 et 4 de la DDHC (C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.*, cons. 8) ; la liberté d'expression est rattachée à l'article 11 de la DDHC (C. const., Décision n° 82-141 DC, 27 juillet 1982, *op. cit.*, cons. 3).

[1303] MONTESQUIEU (C.), *L'Esprit des lois*, *op. cit.*, Livre I : « Ce n'est point le corps des lois que je cherche, mais leur âme ».

par conséquent aux droits et aux libertés qu'elle énonce. Ce terme peut également être ici le synonyme du mot « principe », c'est à dire « ce qui fait la vie d'un État »[1304]. Selon le professeur François Rouvillois, « l'esprit apparait alors comme l'idée directrice, le principe moteur, animateur et organisateur d'une règle ou d'un système »[1305]. Cette définition révèle ainsi que l'« esprit » d'une règle ou d'un système (ici d'une liberté ou d'un droit) se trouve pour l'essentiel dans son origine, ce qui explique la nécessaire récurrence du retour au « point de départ » ou à la « naissance » de la règle ou du système. Dès lors, l'appréhension d'un système ou d'une règle repose sur la connaissance de son élaboration, autrement dit « de savoir par qui, comment, pourquoi et selon quelle logique [le système ou la règle] a été fait »[1306].

508. Les auteurs de la DDHC entendaient édifier « un code universel des droits déclarés pour tous les temps et tous les lieux »[1307] afin de reconnaître une valeur juridique à un ensemble de règles qui soit, selon la thèse des droits naturels, ont toujours existé, soit sont constitutives de droits positifs « créés par la loi, puis sanctionnés par les tribunaux sur le fondement de celle-ci »[1308]. La DDHC constitue ainsi le premier texte français recensant les droits et les libertés de chacun qu'ils soient d'origine « divine » ou issus du droit positif. Du point de vue du droit français, l'être humain existe en tant qu'individu depuis la DDHC de 1789 qui lui reconnait des droits et des libertés opposables à l'État. Aussi, la DDHC ne se contente pas de recenser les règles existantes mais vise à leur octroyer un rang de règles « suprêmes » qui s'élèveraient au-dessus de celles qui chercheraient à y déroger de manière disproportionnée au point de « revenir » à l'Ancien régime. Par ce biais, les constituants inscrivent les principes généraux existants dans un texte qui se veut suffisamment fort afin que les droits et libertés juridiquement reconnus soient tout autant réaffirmés que « protégés » des violations abusives par les pouvoirs publics[1309].

[1304] Définition du terme « principe » issue de *Le Nouveau Petit Littré*, Paris, éditions Garnier, 7ème édition, 2019, p. 1649.

[1305] ROUVILLOIS (F.), *Droit constitutionnel - 1. Fondements et pratiques*, Paris, Flammarion, coll. Champs-Université, 5ème édition, 2001, 435 p., p. 10.

[1306] *Ibid*.

[1307] JAUME (L.), *La Déclaration des droits de l'homme et du citoyen, du débat 1789-1793 au Préambule de 1946*, Paris, Flammarion, 1989, 376 p., p. 19.

[1308] ROUVILLOIS (F.), *Libertés fondamentales*, *op. cit.*, p. 13.

[1309] DDHC, Préambule : « Les représentants du peuple français […] ont résolu d'exposer, dans une Déclaration solennelle, les droits naturels, inaliénables et sacrés de l'homme ».

509. En définitive, la DDHC consistait pour les constituants à exprimer une volonté tant de réaffirmer des règles déjà établies que d'en garantir leurs effets. Néanmoins, la protection et les garanties effectives des droits et libertés énoncés par la DDHC ne résultent pas de leur déclaration par écrit[1310] mais davantage de l'existence d'une organisation juridique et institutionnelle qui s'efforce d'établir des droits objectifs et de les faire respecter. Les droits et libertés simplement énoncés n'ont de valeur opposable à l'arbitraire étatique que lorsque ceux-ci sont élevés au rang de normes ; en d'autres termes, lorsqu'ils sont énoncés par l'État dans des textes comprenant des garanties que ce dernier s'engage à mettre en œuvre et de sanctionner toutes éventuelles atteintes[1311]. L'inscription du droit de ne pas être arbitrairement arrêté ou détenu dans le texte de la DDHC et sa confirmation à l'article 66 de la Constitution de 1958 constitue une garantie concrète de protection de l'individu face aux décisions des autorités publiques. Les termes utilisés pour qualifier ce droit ont évolué depuis 1789 faisant apparaitre au cours du temps un champ plus ou moins large de la notion à laquelle il était rattaché et modifiant dans le même temps les garanties dont il pouvait être assorti (§1).

510. Ces dernières années, la question du droit à la sûreté s'est insérée dans de nombreuses réformes législatives[1312] principalement du fait des évènements à caractère terroriste[1313]. Les dernières législations tendent à confirmer une forme de disparition de l'esprit des textes fondateurs du droit français. En ce sens, les lois relatives au domaine de la sécurité publique ou intérieure, notamment celles en matière de police préventive, échouent à laisser apparaitre un « esprit » ou

---

[1310] Voir en ce sens les réflexions de BARANGER (D.), « *Common Law* et droits de l'Homme », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*, p. 138.

[1311] ROUVILLOIS (F.), *Libertés fondamentales*, *op. cit.*, p. 19.

[1312] Voir notamment : Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue, *JORF* n° 0089 du 15 avril 2011 [en ligne] ; Loi n° 2011-672 du 16 juin 2011 relative à l'immigration, à l'intégration et à la nationalité, *JORF* n°0139 du 17 juin 2011 [en ligne] ; Loi n° 2011-803 du 5 juillet 2011 relative aux droits et à la protection des personnes faisant l'objet de soins psychiatriques et aux modalités de leur prise en charge, *JORF* n°0155 du 6 juillet 2011 [en ligne] ; Loi n° 2013-869 du 27 septembre 2013 modifiant certaines dispositions issues de la loi n° 2011-803 du 5 juillet 2011 relative aux droits et à la protection des personnes faisant l'objet de soins psychiatriques et aux modalités de leur prise en charge, *JORF* n°0227 du 29 septembre 2013 [en ligne] ; Loi n° 2016-274 du 7 mars 2016 relative au droit des étrangers en France, *JORF* n°0057 du 8 mars 2016 [en ligne] ; Loi n° 2018-778 du 10 septembre 2018 pour une immigration maîtrisée, un droit d'asile effectif et une intégration réussie, *JORF* n°0209 du 11 septembre 2018 [en ligne].

[1313] GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* : « dans un contexte "d'obsession" sécuritaire […] marqué par la persistance de la menace terroriste, on voit se développer une inflation de lois destinées soit à prévenir soit à mieux répondre à une éventuelle atteinte à la sécurité de la collectivité ». Voir aussi : TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.* ; GARRIDO (L.),« Le droit à la sûreté : un droit en danger ? » *in* GARRIDO (L.), (dir.), *Le droit à la sûreté : État des lieux, état du droit*, *op. cit.*, p. 3 ; BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *op. cit.* : Évoquant l'adoption d'une conception restrictive de la liberté individuelle par le Conseil constitutionnel, le professeur Guillaume Beaussonie constate « la succession, dans le contexte que nul n'ignore, de lois profondément sécuritaires, dont l'essentiel […] ne s'avère jamais vraiment censuré par le Conseil constitutionnel, jusqu'au paroxysme que constituera l'adoption du projet de loi "renforçant la sécurité intérieure et la lutte contre la terrorisme" ».

même un fondement juridique. En ce sens, le terme de « sécurité » en constitue un parfait exemple puisqu'il s'agit d'une notion éminemment subjective dont les dispositions ne font que répondre aux besoins exprimés par les citoyens sous l'emprise de l'émotion, à l'instar des attentats perpétués en 2015 (§2).

§1. L'évolution de la notion de sûreté vers celle de liberté individuelle

511. La sûreté a vécu des changements tant sur le plan terminologique que s'agissant de son champ d'application. Dès lors, il convient, dans un premier temps, de revenir sur les fondements de la notion de sûreté avant d'aborder celle de la liberté individuelle dont les termes se substituent désormais à celui de sûreté dans la jurisprudence constitutionnelle (A). Ces précisions étant faites, il s'agira, dans un deuxième temps, d'étudier l'évolution du champ de la liberté individuelle au travers des décisions du Conseil constitutionnel et de ses conséquences sur la notion de sûreté (B).

A. Les contours de la notion de sûreté

512. Bien qu'aujourd'hui la notion de sûreté ne soit évoquée que sous les termes de « liberté individuelle » par le juge constitutionnel français, le terme de « sûreté » prévaut au sein des sources européennes et internationales pour décrire le droit de ne pas être arrêté ou détenu arbitrairement par l'État[1314] (1). À cette fin, le droit national et supranational définit les conditions dans lesquelles une personne peut être privée de sa liberté (2).

1. La sûreté, une protection de l'individu contre l'arbitraire étatique

513. Le contenu du droit à la sûreté - La sûreté doit être entendue comme le droit imprescriptible pour toute personne ne pas être arrêtée, ni détenue arbitrairement par l'État[1315]. Paraphrasant le professeur Xavier Bioy, elle constitue le premier principe opposable à l'oppression

[1314] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 695.

[1315] DDHC, art. 2, 7, 8 et 9. Selon le Professeur Jacques Robert : « la notion de sûreté s'éclaire à la lumière des articles 7, 8 et 9 (de la Déclaration des droits de l'homme et du citoyen) qui précisent, l'un que l'accusation, l'arrestation ou la détention d'un individu ne peuvent s'opérer que dans les cas déterminés par la loi et selon les formes qu'elle a prescrites, l'autre, que toute punition ne peut être infligée qu'en vertu d'une loi antérieure fixant des peines strictement et évidemment nécessaires, le troisième, que tout homme est présumé innocent jusqu'à ce qu'il ait été déclaré coupable » (ROBERT (J.), *Liberté publiques*, Paris, Montchrestien, coll. Université nouvelle, Précis Domat, 1971, 651 p., p. 161).

de la puissance publique[1316]. Dans le même sens, les professeurs Dominique Chagnollaud et Guillaume Drago affirment que la sûreté « est incontestablement le premier des droits, chronologiquement et qualitativement, celui par lequel cesse l'arbitraire et s'affirme l'homme libre »[1317]. Le juriste milanais, Cesare Beccaria, était l'un des premiers auteurs à contribuer à définir la notion de sûreté. Il déclarait ainsi que « ce fut […] la nécessité qui contraignit les hommes à céder une partie de leur liberté ; or il est certain que chacun n'en veut mettre à la disposition de la communauté que la plus petite portion possible, mais qui suffise à engager les autres à le défendre. L'ensemble de ces plus petites portions possibles constitue le droit de punir ; tout ce qui s'y ajoute est abus et non justice »[1318]. Il énonce le principe de liberté et l'exception à ce principe nécessaire à l'existence de l'État de droit. Dès lors, la sûreté est la pierre d'angle du droit pénal qui impose que seule la nécessité puisse justifier les restrictions ou les privations de droits ou libertés[1319]. Le droit à la sûreté s'inspire de l'*Habeas Corpus Act* britannique de 1679 qui instaure « le droit de toute personne, s'estimant illégalement détenue, de recourir à un juge afin que celui-ci statue sur la régularité de la détention et ordonne, le cas échéant, sa libération »[1320]. En d'autres termes, la sûreté permet de garantir « la sécurité juridique de l'individu face aux autorités »[1321].

514. Outre la DDHC, le terme de sûreté apparait dans de nombreuses sources internationales et européennes[1322] où il désigne également le droit de chaque personne de ne pas être arrêtée ou détenue de manière arbitraire par l'État. Il convient de noter qu'au sein des textes internationaux, la Conv.EDH est celle qui dispose de la définition la plus étendue et explicite de la sûreté[1323] en son article 5[1324]. En de nombreuses occasions, la CEDH a pris le temps de détailler les modalités

---

[1316] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 695.

[1317] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 685-686.

[1318] BECCARIA (C.), *Dei delitti e delle pene* [*Des délits et des peines*], 1764, §2.

[1319] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 215.

[1320] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 686. Voir aussi : MORANGE (J.), *La déclaration des droits de l'homme et du citoyen*, Paris, PUF, coll. Que sais-je ?, 4ème édition, 2002, 128 p., p. 46 : « La sûreté est extrêmement liée à la liberté puisqu'elle consiste à n'être pas susceptible de faire l'objet d'une poursuite, d'une arrestation ou d'une détention arbitraire. Cette matière, qui faisait l'objet des grands textes du droit anglais, est plus facile à réglementer de façon précise et durable, en droit. Les principes posés aux articles 7, 8, 9 répondent aux préoccupations les plus constantes du XVIIIe siècle ».

[1321] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 275.

[1322] DUDH, art. 3 ; Conv.EDH, art. 5 ; CDFUE, art. 6 ; PIDCP, art. 9.

[1323] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 276 ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 314.

[1324] Conv.EDH, art. 5 : « Toute personne a droit à la liberté et à la sûreté. Nul ne peut être privé de sa liberté, sauf dans les cas [énumérés par le texte] et selon les voies légales ».

d'application de cet article consacré à la liberté et à la sûreté[1325]. Elle insiste sur l'importance émanant du droit à la sûreté dans une « société démocratique » ainsi que sur son caractère inaliénable et exigera un « contrôle scrupuleux » des décisions y portant atteinte[1326]. Parfois, il est même arrivé que la jurisprudence de la CEDH soit contraire à celle des juges français notamment quant à leur conception de la sûreté[1327]. La jurisprudence de la CEDH se différencie principalement par sa constance, adoptant une vision distinguant la privation de liberté de celle de restriction de liberté qu'elle opère en effectuant une analyse du degré ou de l'intensité de l'atteinte à la liberté d'un individu plutôt qu'à la nature de la liberté impliquée[1328]. Ainsi, le respect de la sûreté permet de maintenir l'équilibre entre la liberté propre à chaque individu (tel qu'énoncée à l'article 2 de la DDHC) et les mesures répressives nécessaires à la sauvegarde de l'ordre public. Dès lors, cette liberté n'est pas absolue et « peut subir des contraintes issues des autorités publiques disposant des instruments de répression »[1329]. Le respect de la sûreté de chaque individu repose principalement sur l'application de plusieurs garanties issues du droit pénal.

515. Les principes fondamentaux du droit pénal garants de la sûreté - Le droit à la sûreté agit donc comme une véritable protection de l'individu en garantissant sa sécurité juridique contre l'arbitraire de l'État. Cette garantie s'exprime au travers de plusieurs principes inhérents à la

---

[1325] CEDH, 1er juillet 1961, *Lawless c/ Irlande*, *op. cit.*

[1326] CEDH, 18 juin 1971, *De Wilde, Ooms et Versyp c. Belgique*, *op. cit.*

[1327] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 696 : « Si le Conseil constitutionnel français s'attache à la distinction des peines des autres sources d'atteinte à la liberté, le droit européen envisage l'ensemble des limitations de liberté avec les mêmes exigences. Notre droit distingue la simple "appréhension" qui consiste en la mainmise physique sur l'individu (que peut opérer toute personne sur l'auteur d'une infraction dont il a été témoin en vue de le présenter à un officier de police judiciaire), de l'arrestation qui en constitue l'aspect juridique et ne peut être le fait que de l'autorité compétente » et p. 697 : « La Cour [européenne des droits de l'homme] distingue la privation de liberté qui relève de l'article 2 du Protocole n° 4 qui renvoie à la liberté d'aller et venir » ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 265 : « La Cour européenne des droits de l'homme […] distingue la privation de liberté de la restriction de liberté : la première porte atteinte à la sûreté, la deuxième à la liberté d'aller et venir » ; WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 658 : « Pour la Cour européenne des droits de l'homme, l'arrestation reste incluse dans le champ de l'article 5 de la Convention, comme l'implique la lettre de l'article 5 §1 qui vise "l'arrestation" dans la moitié des causes de privation de liberté qu'il énumère ».

[1328] Voir en ce sens : CEDH, 6 novembre 1980, *Guzzardi c. Italie*, n° 7367/76, spéc. §§ 92-93 [en ligne] et CEDH, 20 avril 2010, *Villa c. Italie*, n° 19675/06, §41 [en ligne].

[1329] OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 315.

procédure pénale[1330] que sont la légalité des délits et des peines[1331], l'interdiction de la rétroactivité de la loi pénale[1332], le droit de ne pas être jugé et puni deux fois pour un même fait (*non bis in idem*)[1333], le respect de la proportionnalité et de la nécessité des sanctions[1334], et la présomption d'innocence (v. **n° 468 et suiv.**). Or, les possibilités d'atteinte à la sûreté sont nombreuses dans le cadre de la procédure pénale et s'opposent à ces principes à commencer par la présomption d'innocence[1335] tel que dans le cadre de l'application des mesures de détention provisoire[1336]. Le recours à des caméras filmant la voie publique tend notamment à amplifier le phénomène d'atténuation du principe de présomption d'innocence en considérant indifféremment les personnes entrant dans le champ de la caméra comme de potentiels suspects susceptibles de commettre une infraction. La sûreté n'étant pas irréfragable, la sauvegarde de l'ordre public peut donc justifier d'y porter atteinte. Néanmoins, ces privations de liberté nécessitent le respect de certaines conditions dont les modalités sont définies au sein du Code de procédure pénale et mis en œuvre sous l'autorité du juge judiciaire.

[1330] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, pp. 704-715 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 332-333 ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 316.

[1331] Ce principe trouve sa source à l'article 8 de la DDHC (« Nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit et légalement appliquée ») et à l'article 34 de la Constitution de 1958 (« La loi fixe les règles concernant [notamment] la détermination des crimes et délits ainsi que les peines qui leur sont applicables »). Il a été confirmé par le Conseil constitutionnel dans sa décision n° 80-127 du 20 janvier 1981 (précédemment citée).

[1332] La non-rétroactivité de la loi pénale est également consacrée à l'article 8 de la DDHC mais aussi à l'article 7 de la Conv.EDH (« Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou international ») ou encore l'article 2 du Code civil (« La loi ne dispose que pour l'avenir, elle n'a point d'effet rétroactif »). Toutefois, ce principe est atténué s'agissant des lois pénales plus douces (HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 333). Ce principe a été, indirectement, rappelé par le juge constitutionnel lors de sa décision relative à la rétention de sûreté en 2008 (C. const., Décision n°2008-562 DC, 21 février 2008, *op. cit.*, cons. 8, 9 et 10).

[1333] Selon la jurisprudence de la CEDH, le principe de *non bis in idem* interdit « de poursuivre ou de juger une personne pour une seconde « infraction » pour autant que celle-ci a pour origine des faits identiques ou des faits qui sont en substances les mêmes » (CEDH, 10 février 2009, *Zolotoukhine c. Russie*, n° 14939/03 [en ligne]).

[1334] Ce principe se fonde sur l'article 8 de la DDHC (« La loi ne doit établir que des peines strictement et évidemment nécessaires ») ainsi que sur l'article 49 de la CDFUE (« L'intensité des peines ne doit pas être disproportionnée par rapport à l'infraction »). Le juge constitutionnel dispose d'un contrôle restreint quant aux choix du législateur mais peut néanmoins faire obstacle à des sanctions qu'il jugerait disproportionnées au regard des faits reprochés (voir en ce sens : C. const., Décision n° 80-127 DC, 20 janvier 1981, *op. cit.*, cons. 13 ; C. const., Décision n° 96-377 DC, 16 juillet 1996, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire*, Rec. p. 87, cons. 7, 8 et 9 [en ligne]).

[1335] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 671.

[1336] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 286 : « La détention provisoire consiste à priver de liberté une personne qui est pourtant présumée innocente » ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 224 : « la détention provisoire heurte de front le principe de la présomption d'innocence » ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 336 : Le recours à la détention provisoire « est relativement fréquent [or] cette pratique limite aussi la portée de la présomption d'innocence toujours affirmée ».

2. Les atteintes permises à la sûreté des individus

516. Les arrestations pouvant mener à une détention - La sûreté, telle qu'énoncée par la DDHC et par le droit européen, entend protéger l'individu contre les arrestations et les détentions arbitraires[1337]. Dans son sens général, l'arrestation peut être définie comme incluant « l'appréhension d'une personne en vue de la poursuivre pénalement, mais également toute mesure mettant une personne à la disposition d'une autorité publique, fut-ce pour un court moment »[1338]. Ainsi que l'énonce la Conv.EDH, aucune arrestation ne peut être reconnue comme étant arbitraire dans les cas relevant de flagrant délit[1339]. En d'autres termes, une arrestation n'est pas reconnue comme étant arbitraire lorsqu'il y a des raisons plausibles de soupçonner qu'une personne arrêtée a commis une infraction. Le respect du droit à la sûreté impose, toutefois, que l'arrestation remplisse certaines obligations au nombre desquelles celle d'un droit pour la personne faisant l'objet d'une arrestation d'être dûment informée des motifs de son arrestation[1340].

517. Toutefois, cette garantie d'information s'est souvent vue fragilisée, notamment dans le cadre des contrôles d'identité[1341] qui, autrefois, étaient considérés comme relevant exclusivement du cadre de la liberté individuelle[1342]. Certains auteurs avaient ainsi fait état du fait que ces contrôles avaient donné lieu à des actes discriminatoires (contrôle au faciès) à de nombreuses reprises incitant le législateur et les juges au débat[1343]. En vue de prévenir les atteintes à l'ordre public, une loi du 2 février 1981, dite « Sécurité et liberté », est venue autoriser la mise en œuvre de contrôles d'identité par la police administrative afin de « prévenir une atteinte à l'ordre public,

---

1337 DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 278 ; CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 685.

1338 WACHSMANN (P.), *Libertés publiques*, *op. cit.*, pp. 658-659.

1339 Conv. EDH, art. 5 §1.

1340 Conv. EDH, art. 5 §2.

1341 Le contrôle d'identité peut être défini comme « l'examen par une autorité de police ou de gendarmerie d'un document de nature à prouver l'identité d'une personne » (ROBERT (J.) et DUFFAR (J.), *Droits de l'homme et libertés fondamentales*, Paris, Montchrestien, 8ème édition, 2009, 908 p., p. 301).

1342 WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 660 : « Il faut souligner que le régime de ces contrôles a été établi à un moment où il ressortissant entièrement de la liberté individuelle, ce qui n'est plus le cas aujourd'hui que de ceux qui relèvent de la police judiciaire ».

1343 HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 336 : « Nombreuses et faiblement encadrées, les opérations de contrôle d'identité suscitent le débat. En effet, les pratiques discriminatoires ou vexatoires auxquelles elles donnent lieu sont régulièrement pointées du doigt » ; WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 668 : « le caractère discriminatoire des contrôles d'identité est une constante ».
Voir aussi : JOBART (F.) et LEVY (R.), Étude « Police et minorités visibles : les contrôles d'identité à Paris », *Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales (CESDIP)*, juillet 2009 [en ligne].

notamment une atteinte à la sécurité des personnes et des biens »[1344]. Les contrôles d'identité peuvent être effectués dans un cadre de police administrative[1345] (à des fins préventives) ou de police judiciaire[1346] (à des fins répressives). Aujourd'hui, seule une vérification d'identité de la personne, des suites d'un contrôle d'identité effectué par la police judiciaire, relève du champ de la liberté individuelle et de la sûreté[1347]. Pour l'heure, l'emploi de caméras « augmentées » de sécurité publique n'a pas vocation à assurer un contrôle d'identité ou une vérification d'identité (tel que par le biais d'une reconnaissance faciale) mais à détecter des situations de danger et notamment, à terme, les individus ayant vraisemblablement commis une infraction[1348] (voir *supra*). Dès lors, si les résultats de l'algorithme d'analyse d'images devaient conduire un agent des forces de l'ordre à prendre la décision d'appréhender le suspect et de le mener devant un officier de police judiciaire, l'arrestation serait alors constitutive d'une privation de liberté qui porterait atteinte à la sûreté de l'individu.

518. Une mesure de détention préalable au jugement, la garde à vue - La sûreté, au même titre que la liberté individuelle, constitue aussi une garantie contre les détentions arbitraires ; en d'autres termes comme « le droit de ne pas être retenu contre son gré en un lieu quelconque »[1349]. Les cas de privation de liberté dans le cadre d'une procédure pénale peuvent advenir avant un jugement ou après un jugement. Le recours à des caméras « augmentées » de sécurité publique est susceptible d'engendrer des cas de privation de liberté précédent un jugement. Il convient donc de

---

[1344] Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes, *JORF* n°0028 du 3 février 1981. Cette loi fut par la suite abrogée et remplacée par la Loi n°83-466 du 10 juin 1983 (portant abrogation ou révision de certaines dispositions de la loi n° 81-82 du 2 février 1981 et complétant certaines dispositions du code pénal et du code de procédure pénale, *JORF* du 11 juin 1983) puis par la Loi n° 93-992 du 10 août 1993 relative aux contrôles et vérifications d'identité, *JORF* n°184 du 11 août 1993 [en ligne].

[1345] CPP, art. 78-2, al. 3.

[1346] CPP, art. 78-2, al. 1er et al. 2.

[1347] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 271 : « Si la vérification d'identité, qui suppose une rétention, porte une atteinte à la sûreté, en revanche, le contrôle d'identité, lui n'est attentatoire qu'à la liberté d'aller et venir » ; WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 670 : « L'hypothèse comportant l'atteinte la plus brève à la liberté individuelle est celle de la vérification d'identité dont peuvent être l'objet les personnes qui, lors d'un contrôle d'identité, ont refusé de ou n'ont pas pu justifier de leur identité ou celles qui n'ont pu satisfaire au relevé de leur identité par un […] officier de police judiciaire ».

[1348] Ces caméras « augmentées » filmant la voie publique pourraient notamment aider à détecter la personne ayant commis une infraction et non celle susceptible de commettre une infraction. Si les finalités de recherche de l'auteur d'une infraction remplissent les conditions de l'objectif de valeur constitutionnelle, celles consistant à anticiper une possible infraction ne rempliraient plus un objectif simplement préventif (objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public) mais « prédictif » qui s'éloigne des finalités de maintien de l'ordre public.

[1349] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 669.

restreindre le propos à une des mesures constitutives d'une privation de liberté pouvant être mise en œuvre préalablement au procès pénal, à savoir la garde à vue[1350].

519. La garde à vue est une mesure de police judiciaire de privation de liberté[1351]. Elle dispose d'une nouvelle définition, depuis une loi du 14 avril 2011[1352], comme étant « une mesure de contrainte décidée par un officier de police judiciaire, sous le contrôle de l'autorité judiciaire, par laquelle une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre un crime ou un délit puni d'une peine d'emprisonnement est maintenue à la disposition des enquêteurs »[1353]. Cette mesure a subi d'importantes réformes suite à la pression exercée conjointement par la CEDH[1354], le Conseil constitutionnel[1355] et, plus tard, par la Cour de cassation[1356]. Depuis la réforme de 2011, cette mesure est désormais soumise à des conditions plus strictes avec des garanties[1357] renforçant la protection de la présomption d'innocence ainsi que les droits des victimes[1358]. Dès lors, elle ne peut être mise en œuvre que dans la mesure où elle constitue l'unique moyen de parvenir à l'un des différents objectifs énumérés par le Code de procédure pénale nécessaires à la réalisation des investigations[1359].

520. À l'occasion d'une question prioritaire de constitutionnalité concernant la loi de réforme de la garde à vue de 2011[1360], le juge constitutionnel avait analysé les dispositions relatives à

[1350] BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, pp. 716-720 ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 279 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 337-340 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, pp. 218-221 et pp. 224-226.

[1351] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 279.

[1352] Loi n° 2011-392 du 14 avril 2011 relative à la garde à vue, *op. cit.*

[1353] CPP, art. 62-2.

[1354] Voir notamment : CEDH, gd. ch., 27 novembre 2008, *Salduz c. Turquie*, n° 36391/02 [en ligne] ; CEDH, 13 octobre 2009, *Dayanan c. Turquie*, n° 7377/03 [en ligne] ; CEDH, 14 octobre 2010, *Brusco c. France*, n° 1466/07 [en ligne].

[1355] C. const., Décision n° 2010-14/22 QPC, 30 juillet 2010, *M. Daniel W. et autres [Garde à vue]*, Rec. p. 179 [en ligne].

[1356] C. cass, ass. plén., 15 avril, 2011, n° 10-17.049 [en ligne].

[1357] Les garanties de la personne gardée à vue sont énumérées aux articles 63-1 et suivants du CPP.

[1358] OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 332.

[1359] CPP, art. 62-2.

[1360] C. const., Décision n° 2011-191/194/195/196/197 QPC, 18 novembre 2011, *Mme Élise A. et autres [Garde à vue II]*, Rec. p. 544 [en ligne].

« l'audition libre » et estimé que celles-ci n'étaient pas contraires aux droits de la défense. Toutefois, il avait émis une réserve d'interprétation exigeant que l' « audition libre » soit autorisée sous la condition que la personne « ait été informée de la nature et de la date de l'infraction qu'on la soupçonne d'avoir commise et de son droit de quitter à tout moment les locaux de la police ou de gendarmerie »[1361]. La loi du 27 mai 2014[1362] a permis au législateur d'adapter le régime de la garde à vue aux exigences du droit européen en transposant la directive européenne relative au droit à l'information dans le cadre des procédures pénales[1363]. Ce renforcement du droit à l'information des personnes est primordial puisqu'il fait référence au principe du contradictoire et plus généralement au droit de la défense inhérent au procès pénal[1364]. Les garanties en matière d'information des personnes mises en garde à vue[1365] ont par la suite été complétées par le législateur lors de l'adoption de la loi du 23 mars 2019 de programmation et de réforme pour la justice 2018-2022[1366]. Toutefois, ce droit à l'information pourrait être affecté par l'arrivée des caméras « augmentées » utilisant des algorithmes d'analyse d'images dont les fonctions principales ne sont pas toujours maitrisées par la population générale (ni parfois par les concepteurs eux-mêmes (v. **n°399-404**)). Dans le cas où les résultats produits par l'algorithme ayant servis à la prise de décision des forces de l'ordre ne seraient pas explicables, cela pourrait constituer une atteinte aux droits de la défense. Dès lors, il s'avère crucial de renforcer les garanties entourant les droits de la défense au regard de cette nouvelle technologie. À cette fin, la mise en œuvre d'une collaboration étroite entre les concepteurs de ces algorithmes, les juristes et les représentants de l'État est essentielle (v. **n° 749 et suiv.**).

521. La garantie que constitue la sûreté pour l'individu, loin d'être irréfragable, pourrait donc encore être réduite par le recours à des technologies d'aide à la prise de décision qui influence les

---

[1361] *Idem*, cons. 19 et 20 : « Toutefois, le respect des droits de la défense exige qu'une personne […] placée en garde à vue, ne puisse être entendue ou continuer à être entendue librement par les enquêteurs que si elle a été informée de la nature et de la date de l'infraction qu'on la soupçonne d'avoir commise et de son droit de quitter à tout moment les locaux de police ou de gendarmerie ».

[1362] Loi n° 2014-535 du 27 mai 2014 portant transposition de la directive 2012/13/UE du Parlement européen et du Conseil, du 22 mai 2012, relative au droit à l'information dans le cadre des procédures pénales, *JORF* n° 0123 du 28 mai 2014 [en ligne].

[1363] Directive (UE) 2012/13/UE du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales, JOUE L142, 1er juin 2012, pp. 1-10 [en ligne].

[1364] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, pp. 285-286.

[1365] CPP, art. 61-1.

[1366] Loi n° 2019-222 de programmation et de réforme pour la justice 2018-2022, 23 mars 2019, *op. cit.* Cette réforme aura également permis d'améliorer l'efficacité des enquêtes en simplifiant la procédure de la mise en garde à vue (BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 718 ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 279).

décisions des forces de l'ordre, sans toujours en comprendre les raisons. Aussi, comme évoqué en introduction, la notion de sûreté est évolutive, sa conception ayant fait l'objet d'une refonte par le Conseil constitutionnel. Aujourd'hui, la jurisprudence ne fait référence qu'à la liberté individuelle pour désigner la sûreté mais ce statut d'équivalence apparent entre les deux notions n'a pas toujours prévalu et son état actuel laisse transparaitre une certaine réduction de la garantie que souhaitaient lui conférer les constituants de 1789.

B. La liberté individuelle comme pendant de la sûreté

522. Si aujourd'hui le droit à la sûreté est considéré comme étant l'unique composante de la liberté individuelle par le juge constitutionnel, il n'en a pas toujours été ainsi. La jurisprudence du Conseil constitutionnel concernant la liberté individuelle a connu des fluctuations en adoptant, dans un premier temps, une conception élargie de son contenu pour, dans un deuxième temps, en rétrécir le champ (1). La notion actuelle de liberté individuelle, comme pendant du droit à la sûreté, laisse néanmoins encore planer le doute quant à son contenu et fait l'objet de débats au sein de la doctrine, dont une partie perçoit une forme d'affaiblissement des garanties posées par les constituants de 1789 pour faire face aux décisions arbitraires de l'État (2).

1. La détermination du champ de la liberté individuelle

523. La notion de liberté individuelle doit être différenciée de celle des libertés individuelles qui rassemblent « l'ensemble des droits fondamentaux de l'individu »[1367]. La liberté individuelle, prise dans son sens actuel, est consacrée à l'article 66 de la Constitution qui dispose que « nul ne peut être arbitrairement détenu », reprenant une partie de ce qui compose le droit à la sûreté. Elle ne revêt pas un caractère irréfragable et peut ainsi faire l'objet de restrictions néanmoins soumises au contrôle de l'autorité judiciaire. Aussi, en dépit des limites qui peuvent lui être imposées, la liberté individuelle présente une valeur capitale aux yeux de la doctrine. En ce sens, de nombreux auteurs estiment que la liberté individuelle, comme la sûreté personnelle, est « beaucoup plus qu'une liberté parmi d'autres, elle est le bouclier de toutes les autres libertés »[1368] permettant de garantir leur

[1367] RENOUX (T.), *Le Conseil constitutionnel et l'autorité judiciaire. L'élaboration d'un droit constitutionnel juridictionnel*, Paris, Économica, coll. Droit public fondamental, Thèse, 1984, 608 p., préf. FAVOREU (L.), p. 514 ; FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, *op. cit.*, p. 476.

[1368] LEBRETON (G.), *Liberté publiques et droits de l'Homme*, *op. cit.*, p. 380 ; RIVERO (J.), « Liberté individuelle et fouille des véhicules », note sous C. const., Décision n° 76-75 DC, 12 janvier 1977, *AJDA* 1978, pp. 215-216.

exercice[1369]. Cependant, la notion de liberté individuelle a subi de nombreux bouleversements sous l'influence des divergences doctrinales[1370] qui expliquent que le Conseil constitutionnel ait longtemps peiné a en déterminer le contenu.

524. La liberté individuelle est une des premières libertés reconnues par le Conseil constitutionnel alors qu'elle n'était pas présente de manière explicite dans le texte de la DDHC[1371]. Pour autant, son fondement constitutionnel se révèle assez tardif, ainsi que l'observe le Président de la Cour de cassation Guy Canivet[1372], puisqu'il apparait bien après l'introduction du contrôle de constitutionnalité[1373] ou encore l'élargissement du bloc de constitutionnalité aux textes inclus dans le préambule de la Constitution de 1958[1374]. Lors de sa décision du 12 janvier 1977, le Conseil constitutionnel a consacré la protection constitutionnelle de la liberté individuelle considérant, en premier lieu, qu'elle « constitue l'un des principes fondamentaux garanties par les lois de la République » et, en deuxième, que « l'article 66 de la Constitution, en réaffirmant ce principe, en confie la garde à l'autorité judiciaire »[1375]. À cet égard, elle dispose d'une double protection en ce qu'elle bénéficie d'une garantie législative, à l'image de tout droit fondamental, ainsi que d'une garantie judiciaire[1376].

[1369] DUGUIT (L.), *Traité de droit constitutionnel - Les libertés publiques*, Tome V, (1925), Paris, Hachette, 2ème édition, 1981, 716 p., p. 6 ; RIVÉRO (J.) et MOUTOUH (H.), *Liberté publiques*, *op. cit.*, n° 37 ; OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 314 ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 275 ; LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme ? », *op. cit.* ; KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *JCl. Libertés*, 20 septembre 2007.

[1370] CANIVET (G.), « Positions et composition dans la genèse d'une liberté fondamentale - Les contours de la liberté individuelle dans la jurisprudence du Conseil constitutionnel », Titre VII, *La liberté individuelle* n° 7, octobre 2021 [en ligne] : « L'évolution de la jurisprudence du Conseil constitutionnel relative à la protection de cette liberté est la résultante de confrontations entre les postures, opinions et théories à l'œuvre dans le mécanisme de détermination de ses décisions ». Voir aussi : DRAGO (G.), « Liberté individuelle et Constitution - Quels principes pour quels juges ? », pp. 529-540 *in Mélanges en l'honneur d'Yves Mayaud - Entre tradition et modernité : le droit pénal en contrepoint*, *op. cit.* ; POTASZKIN (T.), *L'éclatement de la procédure pénale : vers un nouvel ordre procédural pénal ?*, Paris, LGDJ, Thèse, 2014, 579 p., spéc. pp. 310-312.

[1371] C. const., Décision n° 76-75 DC, 12 janvier 1977, *op. cit.*

[1372] CANIVET (G.), « Positions et composition dans la genèse d'une liberté fondamentale - Les contours de la liberté individuelle dans la jurisprudence du Conseil constitutionnel », *op. cit.*

[1373] Introduite par la Constitution de 1958.

[1374] C. const., Décision n° 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association*, *JORF* du 18 juillet 1971, page 7114, Rec. p. 29 [en ligne].

[1375] C. const., Décision n° 76-75 DC, 12 janvier 1977, *op. cit.*, cons. 1 et 2.

[1376] ARMAND (G.), *L'autorité judiciaire, gardienne de la liberté individuelle dans la jurisprudence du Conseil constitutionnel*, Caen, Thèse, 2000, p. 145.

525. À l'origine, le juge constitutionnel avait adopté une conception élargie de la liberté individuelle, laquelle incluait tant la prohibition des arrestations et détentions arbitraires[1377] (de l'article 66 de la Constitution) que la liberté d'aller et venir[1378], le droit au respect de la vie privée[1379], la protection des données personnelles[1380] ou encore l'inviolabilité du domicile[1381]. Ainsi, les atteintes à ces libertés rassemblaient des objectifs relevant tant de la police judiciaire que de la police administrative. Cette conception large reposait sur une volonté des Sages d'octroyer un fondement constitutionnel à d'autres libertés[1382]. Pour certains auteurs, cette conception étendue de la liberté individuelle, incluant le droit au respect de la vie privée et la liberté d'aller et venir, est ce qui a permis au Conseil constitutionnel de censurer le texte qui avait été déféré à son contrôle[1383]. Par la suite, le juge constitutionnel avait confirmé cette conception de la liberté individuelle[1384] lui rattachant la liberté d'aller et venir[1385] ainsi que le droit au respect de la vie privée[1386]. Plus tard, il abandonna cette position pour lui préférer une vision plus restreinte de la notion de liberté individuelle. En dépit de cette conception restrictive de la liberté individuelle désormais adoptée par

---

[1377] Voir notamment : C. const., Décision n° 79-109 DC, 9 janvier 1980, *Loi relative à la prévention de l'immigration clandestine*, Rec. p. 29, cons. 4 [en ligne] ; C. const., Décision n° 80-127 DC, 20 janvier 1981, *op. cit.*, cons. 56 ; C. const., Décision n° 86-213 DC, 3 septembre 1986, *Loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État*, Rec. p. 122, cons. 17 [en ligne] ; C. const., Décision n° 89-260 DC, 28 juillet 1989, *Loi relative à la sécurité et à la transparence du marché financier*, Rec. p. 71, cons. 6 [en ligne] ; C. const., Décision n° 91-294 DC, 25 juillet 1991, *Loi autorisant l'approbation de la convention d'application de l'accord de Schengen du 14 juin 1985*, Rec. p. 91, cons. 40 [en ligne].

[1378] Voir notamment : C. const., Décision n° 92-307 DC, 25 février 1992, *Loi portant modification de l'ordonnance n° 45-2658 du 2 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France*, op. cit., cons. 13 ; C. const., Décision n° 93-323 DC, 5 août 1993, *Loi relative aux contrôles et vérifications d'identité*, Rec. p. 213, cons. 11, 15 et 16 [en ligne] ; C. const., Décision n° 93-325 DC, 13 août 1993, *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*, *op. cit.*, cons. 3.

[1379] C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 3.

[1380] C. const., Décision n° 93-325 DC, 13 août 1993, *op. cit.*, cons. 133.

[1381] C. const., Décision n° 83-164 DC, 29 décembre 1983, *Loi de finances pour 1984*, Rec. p. 67, cons. 28 [en ligne] : « Considérant cependant que, si les nécessités de l'action fiscale peuvent exiger que des agents du fisc soient autorisés à opérer des investigations dans des lieux privés, de telles investigations ne peuvent être conduites que dans le respect de l'article 66 de la Constitution qui confie à l'autorité judiciaire la sauvegarde de la liberté individuelle sous tous ses aspects, et notamment celui de l'inviolabilité du domicile ».

[1382] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 687 ; FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, pp. 201-202 ; BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 699 ; PERERA (S.), *Le principe de liberté en droit public français*, *op. cit.*, p. 174.

[1383] FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, *op. cit.*, n° 31, §8, pp. 476-477. Voir aussi : RENOUX (T.), *Le Conseil constitutionnel et l'autorité judiciaire. L'élaboration d'un droit constitutionnel juridictionnel*, *op. cit.*, p. 519 et suiv.

[1384] CANIVET (G.), « Positions et composition dans la genèse d'une liberté fondamentale - Les contours de la liberté individuelle dans la jurisprudence du Conseil constitutionnel », *op. cit.*

[1385] C. const., Décision n° 93-325 DC, 13 août 1993, *op. cit.*, cons. 3.

[1386] C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 3 : « la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle ».

le Conseil constitutionnel, sa conception étendue reste défendue par de nombreux auteurs[1387] dont certains ont été membres du Conseil constitutionnel[1388].

526. Depuis le 16 juin 1999[1389], le Conseil constitutionnel adopte une définition plus étroite de la liberté individuelle en limitant celle-ci à la seule protection contre la détention arbitraire, se rapprochant du champ du droit à la sûreté. Dans sa décision du 19 janvier 2006, le juge constitutionnel a ainsi donné une définition restrictive de la liberté individuelle, semblable à celle du droit à la sûreté, « selon laquelle nul ne peut être arbitrairement détenu »[1390]. Ce faisant, il a restreint le contenu de la liberté individuelle aux seules privations de liberté (physique), tel qu'énoncé par l'article 66 de la Constitution de 1958, qui regroupent l'ensemble des mesures prises dans le cadre d'une procédure pénale[1391]. En d'autres termes, toute détention, y compris une rétention ou une retenue de quelques heures de l'individu précédemment arrêté ou appréhendé, constitue une atteinte à la liberté individuelle ou au droit à la sûreté[1392]. Aujourd'hui, la sûreté peut donc être reconnue comme étant synonyme de la liberté individuelle[1393]. Les autres libertés qui y étaient rattachées ont été transférées au sein d'une même notion de liberté personnelle avant d'être individualisées sur le fondement des article 2 et 4 de la DDHC[1394]. Ce n'est donc qu'après de longues tergiversations jurisprudentielles que la liberté individuelle sera finalement rattachée aux articles 2 et 7 de la DDHC.

[1387] Tels que le Professeur François Luchaire (voir notamment : LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme, *op. cit.*, pp. 617 et suiv.) ou encore le Professeur Jean Rivero (voir en ce sens : RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome I, *op. cit.*, p. 28 : « On classe souvent cette liberté fondamentale parmi les libertés de la personne physique, en raison de son aspect le plus voyant : la certitude, pour les citoyens, qu'ils ne feront pas l'objet, notamment de la part du pouvoir, de mesures arbitraires les privant de leur liberté matérielle, telles qu'arrestation ou détention. En réalité, la notion de sûreté est plus large : au-delà même de la privation de la liberté physique, elle condamne toute forme arbitraire de répression »).

[1388] KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *op. cit.*, §2.

[1389] C. const., Décision n° 99-411 DC, 16 juin 1999, *op. cit.*, cons. 2 : « Il appartient au législateur d'assurer la conciliation entre [l]es objectifs de valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent notamment la liberté individuelle et la liberté d'aller et venir ».

[1390] C. const., Décision n° 2005-532 DC, 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, *op. cit.*, cons. 16.

[1391] C. const. Décision n° 2004-492 DC, 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, Rec. p. 66, cons. 3 et 6 [en ligne].

[1392] KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *op. cit.*, §3.

[1393] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 687 ; DELVOLVÉ (P.), « Sécurité et sûreté », *op. cit.* : La sûreté serait « intrinsèquement la liberté individuelle, et inversement ».

[1394] Pour la liberté d'aller et venir et le droit à la vie privée : C. const., Décision n° 2003-467 DC, 13 mars 2003, *Loi pour la sécurité intérieure*, Rec. p. 211, cons. 8 [en ligne] : « la liberté d'aller et venir et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

2. Les contours du champ de la liberté individuelle et de la sûreté

527. Le champ de la liberté individuelle fait encore l'objet de critiques de la part de certains membres de la doctrine qui perçoivent un appauvrissement des garanties que procurait initialement la sûreté (a). Aussi, la distinction entre la liberté individuelle et la liberté d'aller et venir, autrefois en symbiose, nécessite un examen minutieux des autorités juridictionnelles[1395], nationales comme européennes (b).

a. Les critiques d'une conception trop restrictive de la sûreté

528. La conception étroite du champ de la liberté individuelle adoptée par le Conseil constitutionnel qui la relie à la notion de sûreté suscite encore des débats au sein de la doctrine. Certains auteurs la perçoivent comme un « amoindrissement des garanties »[1396] contre les atteintes aux libertés. Dans sa conception étendue, la liberté individuelle recouvre un ensemble de libertés qui, outre la sûreté individuelle, inclut la liberté d'aller et venir et l'inviolabilité du domicile ainsi que le droit à la vie privée[1397]. Pour certains auteurs, la garantie contre les détentions arbitraires constitue l'essence du régime de sûreté et conditionne l'existence de la liberté individuelle[1398]. Toutefois, ils refusent l'interprétation limitant le contenu de la liberté individuelle au premier alinéa de l'article 66 de la Constitution de 1958 relatifs aux seules détentions arbitraires[1399]. Ainsi, le professeur François Luchaire dénonce une diminution progressive de la protection qu'assure la sûreté aux individus[1400]. En ce sens, il démontre que les Révolutionnaires avaient envisagé la sûreté comme une « garantie de droit » avant que celle-ci ne soit interprétée uniquement comme une « garantie de l'ordre » pour ensuite être perçue comme seule « garantie des moyens d'existence »

1395 Voir notamment : ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, Paris, LGDJ, 12ème édition, 2020, 1039 p., p. 723 : « le Conseil constitutionnel est conduit à opérer des distinctions subtiles, souvent justifiées mais parfois aléatoires, afin de déterminer le champ exact de la liberté individuelle ».

1396 WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 655.

1397 BURDEAU (G.), *Libertés publiques,* Paris, LGDJ, 4ème édition, 1972, 458 p., p. 111 : « juridiquement, [la liberté individuelle] s'analyse dans une triple prérogative, dont le respect conditionne l'exercice de toutes les autres libertés : a) liberté d'aller et venir, de s'installer, de quitter sa résidence, sous les seules réserves imposées par l'ordre public ; b) sûreté individuelle qui exige que nul ne puisse être arrêté ou détenu que dans les cas suivants les formes prévues par la loi ; c) liberté de l'intimité que concrétise l'inviolabilité du domicile et de la correspondance ».

1398 RENOUX (T.), *Le Conseil constitutionnel et l'autorité judiciaire. L'élaboration d'un droit constitutionnel juridictionnel*, *op. cit.*, p. 523.

1399 POTASZKIN (T.), *L'éclatement de la procédure pénale : vers un nouvel ordre procédural pénal ?*, *op. cit.*, p. 311.

1400 LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme », *op. cit.*, pp. 617 et suiv.

pour *in fine* en être réduite au rang de « sûreté attrape-tout » unique garantie contre l'arbitraire[1401].

529. D'autres auteurs s'élèvent également contre cette réduction du champ de la liberté individuelle[1402]. En ce sens, le professeur Jean Rivero dénonçait le fait que la sûreté se trouve souvent classée parmi les libertés de la personne physique comme la simple certitude pour les citoyens « qu'ils ne feront pas l'objet notamment de la part du pouvoir, de mesures arbitraires les privant de leur liberté matérielle, telles qu'arrestations ou détention »[1403]. Les défenseurs d'une conception élargie de la sûreté arguent que cette liberté, qui avait pourtant tout son sens lors de son inscription dans la DDHC de 1789, fait l'objet d'une interprétation trop restreinte. Ils soutiennent qu' « en réalité, la notion de sûreté est plus large : au-delà même de la privation de liberté physique, elle condamne toute forme arbitraire de la répression »[1404]. À ce titre, le professeur Jean Rivero démontrait que l'article 7 de la DDHC comprend une double dimension où les termes « arrêté » et « détenu » renvoient certes à une conception étroite et physique de la sûreté (telle qu'elle est interprétée aujourd'hui) mais où le terme « accusé » renvoie à une vision plus étendue de la protection contre l'arbitraire en général[1405]. En se référant au texte d'origine de la sûreté énoncé par la DDHC, le constat est fait que celle-ci ne se limite pas simplement au droit de ne pas être arrêté ou détenu de manière arbitraire mais qu'elle exige aussi, selon Montesquieu, « que le gouvernement soit tel qu'un citoyen ne puisse craindre un autre citoyen »[1406]. En d'autres termes, cela signifie que l'intention originelle des rédacteurs de la DDHC était de protéger le citoyen contre le fait même d'être suspecté à tort ou arbitrairement par l'État.

530. La volonté des constituants de préserver toute personne d'être arbitrairement soupçonnée par l'État se reflète au cœur du principe de la présomption d'innocence inhérent au droit pénal. Cette conception de la sûreté va dans le sens que lui confèrent Messieurs Robert et Duffar qui

---

[1401] *Ibid.*

[1402] Voir notamment : LAZERGES (C.) et ROUSSEAU (D.), Commentaire sous décision C. const., Décision n° 2003-467 DC, 13 mars 2003, 2003 [en ligne]. Les auteurs affirment que « la liberté individuelle est un concept générique qui ne vaut rien - ou presque - sans sa déclinaison en liberté individuelles : la sûreté personnelle, la liberté d'aller et venir, l'inviolabilité du domicile, le respect de la vie privée, … Ce sont ces libertés-là, concrètes et pratiques, qui forment la liberté individuelle et qui doivent à ce titre, bénéficier de la surveillance de l'autorité judiciaire ».

[1403] RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome II, *op. cit.*, p. 23.

[1404] Voir en ce sens : *Ibid* ; RENOUX (T.), *Le Conseil constitutionnel et l'autorité judiciaire. L'élaboration d'un droit constitutionnel juridictionnel*, *op. cit.*, p. 514 et suiv.

[1405] RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome I, *op. cit.*, p. 28.

[1406] MONTESQUIEU, *L'esprit des lois*, *op. cit.*, Livre XI, Chapitre VI.

rappellent qu'elle inclut également le principe de légalité des délits et des peines ainsi que le droit à un procès équitable[1407]. Il ne s'agit par conséquent non pas d'une simple conception matérielle mais également « morale » de l'arbitraire de l'État[1408]. Cette conception « morale », cet « esprit » dont disposait les textes originaux qui forge le droit constitutionnel français s'est estompé avec l'introduction des lois successives relatives à la sécurité (publique ou intérieure). Le recours à des caméras filmant l'espace public, notamment, tend à réduire cette dimension « morale » de la sûreté en suscitant une forme de suspicion généralisée qui agit sur les comportements des personnes filmées (v. **n° 323-327**) et dont les effets pourraient être accentués par l'association à ces caméras d'algorithmes d'analyse d'images. De fait, les algorithmes d'analyse d'images qui permettraient un suivi d'individus pourraient présenter des résultats qui déformeraient la réalité conduisant à des accusations arbitraires voire à des détentions arbitraires. Dès lors, cette conception restreinte de la sûreté, qui coïncide avec la politique sécuritaire des années 1990[1409], affecte les garanties qui lui étaient originairement conférées. La sûreté semble ainsi avoir perdu une partie de sa substance en limitant ses garanties à la seule protection contre les détentions arbitraires[1410] et non plus contre de potentielles accusations arbitraires de la puissance publique[1411].

531. Si la limitation de la protection contre la suspicion arbitraire que semblait assurer la sûreté est contestable, la conception restrictive de la liberté individuelle aux seules détentions arbitraires a néanmoins permis de rejoindre la conception de ce droit décrite par l'article 5 de la Conv.EDH[1412]. En outre, la position adoptée par le juge constitutionnel depuis sa décision de 1999 a favorisé l'émancipation des libertés qui étaient anciennement rattachées à la liberté individuelle,

---

[1407] ROBERT (J.) et DUFFAR (J.), *Droits de l'homme et libertés fondamentales*, *op. cit.*, p. 300.

[1408] Le professeur Louis Favoreu rappelait ainsi que la notion de sûreté disposait d'une double signification dont l'une était celle d'une « garantie générale contre toute forme d'arbitraire » et affirmait ainsi qu' « il ne [pouvait] y avoir de démocratie, si le citoyen évite d'exprimer ses opinions politiques et religieuses, tait ses comportements personnels et privés par peur des représailles que les autorités publiques pourraient engager contre lui » (FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, *op. cit.*, p. 204).

[1409] En ce sens, les premières caméras de surveillance de l'espace public sont apparues dans les années 1990 et la réduction du champ de la liberté individuelle aux seules détentions arbitraires par le juge constitutionnel est issue d'une décision de 1999.

[1410] BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *op. cit.* : « en adoptant […] une vision trop modeste de la liberté individuelle au sens [de l'article 66 de la Constitution] les "Sages" semblent […] faire de la liberté individuelle la seule interdiction d'une détention arbitraire, à laquelle il paraît avoir assimilé la sûreté, le "juge" constitutionnel a rendu possible la détermination d'un régime moins protecteur pour toutes les libertés qui, selon lui, ne ressortissent plus à la sûreté dans un sens désormais restreint ».

[1411] Voir la rédaction de l'article 7 de la DDHC.

[1412] KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *op. cit.*, §3.

d'une part, et d'éviter dans le même temps une « dégradation de sa protection »[1413] en associant la sûreté individuelle à d'autres libertés[1414]. Enfin, cette redéfinition du champ de la liberté individuelle a conduit à un certain renforcement du régime constitutionnel[1415] dans la mesure où les lois portant atteinte à la liberté individuelle font l'objet d'un contrôle constitutionnel de proportionnalité[1416] (v. **n° 851**).

b. La distinction ténue entre mesures restrictives et privatives de liberté

532. Ainsi que le rappellent les professeurs Dominique Chagnollaud et Guillaume Drago, « la notion de sûreté ne doit pas être confondue avec celle de liberté d'aller et venir »[1417]. Les deux notions se distinguent par le fait que la sûreté porte sur une privation de liberté et que la liberté d'aller et venir se limite à protéger une restriction de liberté[1418]. Dès lors, si toute privation de liberté constitue une entrave à la liberté d'aller et venir, toute restriction de cette liberté ne porte pas nécessairement atteinte à la sûreté[1419]. Cette distinction est clairement posée par l'article 5 de la Conv.EDH où l'arrestation ne concerne qu' « un instant dans le temps » tandis que la détention induit « un étalement dans ce temps »[1420]. La décision *Guzzardi c. Italie* avait permis à la CEDH de préciser que « pour déterminer si un individu se trouve "privé de sa liberté" au sens de l'article 5, il

---

[1413] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 687.

[1414] En ce sens, le professeur Louis Favoreu affirmait que la liberté individuelle « ne devait pas être appréhendée comme un ensemble de libertés mais comme le point de rencontre de certaines d'entre elles lorsque pèse sur ces dernières un certain degré de contrainte qui les fait alors basculer dans le champ de la liberté individuelle » (FAVOREU (L.) *et al.*, *Droit constitutionnel*, Paris, Dalloz, coll. Précis, 24ème édition, 2021, 1200 p., n° 1283).

[1415] ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 724, n° 1017 : « En contrepartie du recentrage de la notion de liberté individuelle sur la notion de sûreté, le régime constitutionnel est renforcé. […] en présence d'une mesure privative de liberté, les atteintes portées par le législateur à la liberté individuelle, comme celles portées à la liberté d'aller et venir et au respect de la vie privée, doivent être "adaptées, nécessaires et proportionnées aux objectifs poursuivis", ce triple test de proportionnalité attestant du niveau le plus intense du contrôle exercé par le Conseil constitutionnel ».

[1416] C. const., Décision n°2008-562 DC, 21 février 2008, *op. cit.* Voir aussi : C. const., Décision n° 2010-71 QPC, 26 novembre 2010, *Mlle Danielle S.*, Rec. p. 343, cons. 14 et 16 [en ligne] ; C. const., Décision n° 2016-536 QPC, 19 février 2016, *Ligue des droits de l'homme*, *JORF* n°0044 du 21 février 2016, n° 27, cons. 4 [en ligne].

[1417] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 688.

[1418] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 265 ; CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 4.

[1419] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 688 ; DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 373 ; BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 732.

[1420] KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *op. cit.*, §12.

faut partir de sa situation concrète et prendre en compte un ensemble de critères comme le genre, la durée, les effets et les modalités d'exécution de la mesure considérée »[1421].

533. La frontière entre l'arrestation et la détention est donc ténue[1422] comme l'énonçait la CEDH précisant que « la distinction à établir entre privation et restriction de liberté n'est que de degré ou d'intensité, non de nature ou d'essence »[1423]. Afin d'y remédier, plusieurs éléments d'identification ont été progressivement avancés. Ainsi, le juge constitutionnel a recours à des critères d'objet (ex. garde à vue), de durée et d'effets[1424]. La CEDH a, elle aussi, isolé des critères d'identification notamment dans le cadre d'une affaire concernant les zones de transit[1425]. Il est possible de distinguer « une mesure restrictive de liberté lorsque le degré de contrainte qui pèse sur la liberté d'aller et venir n'est pas de nature à en empêcher totalement l'exercice »[1426]. Dans le cas d'un usage de caméras de surveillance « augmentées » de sécurité publique, la frontière se situerait entre le moment où la personne suspectée est arrêtée afin de vérifier si le résultat de l'algorithme d'analyse d'images est correct et le moment où celle-ci est conduite au poste de police ou de gendarmerie nationale.

534. Les résultats produits par les caméras « augmentées » de sécurité publique pourraient sensiblement modifier le processus décisionnel des forces de l'ordre et fragiliser la frontière qui distingue encore l'arrestation de la détention. Néanmoins, si l'intégration des algorithmes d'analyse d'images à des caméras de vidéoprotection n'est pas anodine, ces technologies entendent contribuer au respect de la sûreté en limitant les alertes aux forces de l'ordre à des situations préétablies lors des phases d'apprentissage. Les alertes émises par ces algorithmes ne concerneraient que des

---

[1421] CEDH, 6 novembre 1980, *Guzzardi c. Italie*, n° 7367/76, *op. cit.*, §92.

[1422] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 4 : La distinction entre mesures restrictives et mesures privatives de liberté reflète « la difficile articulation entre le principe de compétence judiciaire en matière de liberté individuelle et le principe de séparation des autorités administratives et autorités judiciaires qui a conduit le juge constitutionnel à redéfinir les relations entre la liberté individuelle et la liberté d'aller et venir ». Cependant, « la frontière entre ces catégories de mesures peut parfois être délicate à poser ».

[1423] CEDH, 6 novembre 1980, *Guzzardi c. Italie*, n° 7367/76, *op. cit.*, §93.

[1424] Voir en ce sens : C. const., Décision n° 92-307 DC, 25 février 1992, *op. cit.*, cons. 15, 16 et 17 : « Le maintien d'un étranger en zone de transit, en raison de l'effet conjugué du degré de contrainte qu'il revêt et de sa durée, a néanmoins pour conséquence d'affecter la liberté individuelle de la personne qui en fait l'objet au sens de l'article 66 de la Constitution ».

[1425] CEDH, 25 juin 1996, *Amuur c. France*, n°19776/92, §42 [en ligne].

[1426] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, p. 4. Voir en ce sens : C. const., Décision n° 99-411, 16 juin 1999, *op. cit.*

situations où il serait légitime de penser qu'un individu a commis une infraction ou encore lorsqu'une personne est recherchée et qu'elle correspond au profil de l'individu observé.

535. Les développements précédents démontrent que la sûreté est une garantie pour toutes les libertés individuelles. Pour autant, celle-ci n'est pas intangible. En ce sens, le professeur Adhémar Esmein déclarait que « quelque légitime que soient les droits individuels [issus de la DDHC] ils n'ont pas une portée illimitée. Ils ont au contraire deux limites nécessaires : le respect du droit égal chez autrui et le maintien de l'ordre public »[1427]. Aussi, la sûreté a été fragilisée par les transformations terminologiques qui lui ont préféré les termes de liberté individuelle. Or, il se pourrait que cette atténuation de l'emploi de la notion de sûreté soit à l'origine de sa confusion avec le terme de sécurité.

§2. L'introduction de la sécurité en substitution de la sûreté

536. La sûreté, pourtant placée au plus haut rang dans la DDHC (article 2) et constitutionnalisée de longue date[1428], a été progressivement détrônée par la « sécurité » dont la Constitution ne fait pourtant pas mention, sauf à la rattacher à la notion d'ordre public[1429] mentionnée à l'article 10 de la DDHC. En d'autres termes, la « sécurité » semble s'imposer au sein de la législation en dépit d'une absence d'existence explicite au sein du bloc de constitutionnalité. Aussi, le terme de « sécurité » se substitue progressivement à la notion d'ordre public qui, pourtant, fait l'objet de deux objectifs de valeur constitutionnelle[1430] (A).

537. Le droit français, qui dans l' « esprit » des rédacteurs de la DDHC reposait notamment sur un concept objectif de sûreté en cas d'atteinte aux libertés (ordre public), semble lentement

---

[1427] ESMEIN (A.), *Éléments de droit constitutionnel français et comparé*, Paris, Sirey, tome I, 8ème édition, 1921, 1286 p., p. 600 [en ligne]. Dans le même sens, le professeur Jacques Moreau déclarait s'agissant de la liberté individuelle (comprise comme synonyme de la sûreté) qu'elle « n'a pas une valeur absolue, qui existerait en soi, mais elle est l'élément central d'une synthèse entre deux impératifs : le respect des libertés et la préservation de l'ordre public » (MOREAU (J.), « La liberté individuelle dans la jurisprudence du Conseil constitutionnel » *in Renouveau du droit constitutionnel. Mélanges en l'honneur de Louis Favoreu*, Paris, Dalloz, 2007, 1783 p., p. 1661.

[1428] C. const., Décision n° 76-75 DC, 12 janvier 1977, *op. cit.*

[1429] Voir en ce sens la décision du Conseil constitutionnel qualifiant d'objectif de valeur constitutionnelle la prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, et à la recherche des auteurs d'infractions (C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*).

[1430] Voir ci-avant pour la prévention des atteintes à l'ordre public et voir C. const., Décision n° 82-141 DC, 27 juillet 1982, *op.* cit. pour la sauvegarde de l'ordre public.

basculer au profit de ce concept de sécurité purement pratique et subjectif[1431] qui repose autant sur la prévention que sur la répression. En ce sens, les effets induits par la peur d'attaques terroristes ont conduit le législateur à adopter de manière impulsive de nombreuses lois à visée sécuritaire[1432] (B).

A. La corrélation entre sûreté et ordre public comme fondement de l'État de droit

538. L'appréciation des fondements du rapport entre sûreté et sécurité repose sur une perception claire des pouvoirs de police et de l'étendue du champ que recouvre l'ordre public. La conciliation entre la sûreté et l'ordre public apparait distinctement au travers de l'article 10 de la DDHC qui définit une limite aux droits et libertés dès lors qu'apparait un trouble à l'ordre public[1433]. Cette conciliation se trouve au cœur de la police (pris dans son sens étendu)[1434]. De fait, la police a pour mission d'assurer la sécurité publique, notion inhérente à l'ordre public, qui repose sur « le maintien de l'ordre public, la sécurité des personnes et la sauvegarde des biens »[1435]. Le terme de *police* tient son origine étymologique du grec *polis* qui signifie la cité, en d'autres termes l'État libre et souverain. À ce titre, la « liberté » de l'État suppose que la police, chargée de maintenir la bonne administration de la cité, ne devrait « être sollicitée qu'avec réserve »[1436]. Dans sa définition de la police, le professeur Étienne Picard rappelle que son exercice est soumis à des principes essentiels énonçant que les limites qu'elle inflige aux droits et libertés ne sauraient être

---

[1431] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 84 : « le passage de la "sûreté" à la "sécurité" n'est pas qu'un simple glissement sémantique […] alors que la sûreté désigne une situation objective, une tranquillité, l'absence de trouble, la sécurité renvoie à un sentiment subjectif ».

[1432] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, pp. 17-18 : « Confrontés à des menaces nouvelles (des attentats terroristes, des troubles dans les banlieues, ou encore des épidémies […]), les États ont une dangereuse tendance a y répondre par des mesures de circonstances attentatoires aux libertés, mais spectaculaires, c'est-à-dire donnant à l'opinion publique l'impression d'une riposte adaptée […]. De telles mesures grignotent insidieusement les libertés et affaiblissent la vigilance des citoyens, quand elles ne sont pas accueillies par eux avec soulagement ».
Voir aussi en ce sens : Annexe 3 qui démontre qu'une loi à visée sécuritaire est adoptée environ chaque année.

[1433] Pour rappel, l'article 10 de la DDHC énonce que : « nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi ».

[1434] TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 307 : « La contradiction entre liberté et ordre public est l'essence même de la police ; son objet est précisément de la transformer en conciliation ».

[1435] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 853.

[1436] PÉTOT (X.) et ZACHARIE (C.), *La police administrative*, *op. cit.*, p. 12. Voir aussi : PETIT (J.) et FRIER (P-L.), *Droit administratif*, Paris, LGDJ, 2022, 812 p., pp. 361-362 : « la police générale, dans un État libéral, ne doit intervenir que dans de rares hypothèses ».

arbitraires sans contrevenir à l'État de droit[1437]. La notion d'arbitraire doit être comprise comme toute restriction aux droits et libertés « inspirée par la seule subjectivité, le seul caprice ou la seule fantaisie de l'autorité qui les décide »[1438]. Les limites opposées aux droits et libertés doivent par conséquent reposer sur des motifs objectifs tenant à l'ordre public.

539. Sous l'Ancien Régime, les pouvoirs attribués à la police s'inscrivent dans le contexte particulier de la monarchie absolue et traduisent l'existence « d'un État paternaliste et d'un pouvoir personnel qui entendent administrer l'ordre, discipliner les comportements sociaux, structurer l'espace et le temps, imposer une police des consciences et des mœurs, apporter le bien-être, dispenser le bonheur »[1439]. La Révolution française illustre une tout autre approche de la conception et de la gestion de l'État dans la mesure où les constituants visaient un objectif d'équilibre entre l'exigence de sauvegarde de l'ordre public, d'une part, et la garantie des libertés, d'autre part[1440]. En ce sens, la DDHC du 26 août 1789 énonce que « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme »[1441] comprenant « la liberté, la propriété, la sûreté et la résistance à l'oppression »[1442]. Ainsi, les constituants ont érigé la liberté au rang de principe induisant que toute mesure venant en limiter l'expression (mesures d'ordre public) en constitue l'exception.

540. Dans la continuité de cet esprit, le Conseil d'État a consacré les principes propres à l'ordre public dans l'arrêt *Baldy* rendu le 10 août 1917[1443]. À cette occasion, le commissaire au gouvernement Corneille est venu rappeler que « la liberté est la règle, et la restriction de police l'exception » décrivant ainsi le principe de résolution du conflit entre autorité publique et

---

[1437] PICARD (É.), « La police », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, p. 1168.

[1438] *Ibid*.

[1439] PLESSIX (B.), *Droit administratif général*, *op. cit.*, n° 281.

[1440] PÉTOT (X.) et ZACHARIE (C.), *La police administrative*, *op. cit.*, p. 14.

[1441] DDHC, art. 1er.

[1442] DDHC, art. 2.

[1443] CE, 10 août 1917, n°59855, *Baldy*, Rec. p. 638.

libertés[1444]. Aussi, le développement du contrôle juridictionnel a permis de garantir le maintien de la liberté au rang de principe sur les pouvoirs de police dont l'exercice a été défini par le Conseil d'État dans l'arrêt *Benjamin*[1445]. Le principe fut également confirmé dans l'arrêt *Daudignac*[1446] où le juge administratif a conclu à l'inadmissibilité des dispositions législatives mettant en place une interdiction générale et absolue[1447]. De même, le Conseil d'État a renouvelé sa position issue de l'arrêt *Benjamin* dans un arrêt *Naud* du 23 janvier 1953[1448]. Dès lors, les libertés ne peuvent subir d'autres restrictions de la part des autorités publiques que celles strictement nécessaires en vue de garantir l'ordre public.

541. Les libertés et l'ordre public sont étroitement liés, leur existence commune étant aussi essentielle que complexe à maintenir[1449]. La sauvegarde de l'ordre public permet l'exercice des libertés et, de manière corollaire, l'absence de libertés ôte tout objet à l'ordre public[1450]. Dès lors, leur existence repose sur le maintien d'un certain équilibre où l'ordre public n'interviendrait que lorsque l'exercice des libertés est mis en péril[1451]. Cette corrélation est clairement énoncée aux articles 4 et 5 de la DDHC[1452]. Ainsi, l'ordre public consiste autant à protéger les libertés qu'à en

---

[1444] *Ibid* : « Pour déterminer l'étendue du pouvoir de police dans un cas particulier, il faut toujours se rappeler que les pouvoirs de police sont toujours des restrictions aux libertés des particuliers, que le point de départ de notre droit public est dans l'ensemble les libertés des citoyens, que la déclaration des droits de l'homme est implicitement ou explicitement au frontispice des Constitutions républicaines, et que pour toute controverse de droit public doit, pour se calquer sur les principes généraux, partir de ce point de vue que la liberté est la règle et la restriction de police l'exception ».

[1445] CE, 19 mai 1933, n° 17413, *Benjamin*, Rec. 541 [en ligne] : À cette occasion le juge administratif avait précisé que « s'il incombe au maire de prendre les mesures qu'exige le maintien de l'ordre, il doit concilier l'exercice de ses pouvoirs avec le respect de la liberté de réunion ».

[1446] CE, ass., 22 juin 1951, n° 00590 02551, *Daudignac*, Rec. p. 362 [en ligne].

[1447] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 362.

[1448] CE, sect., 23 janvier 1953, *Naud*, Rec. p. 32.

[1449] Voir notamment : WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 65 ; BURG (M.), *Droit fondamental et opérationnel du maintien de l'ordre public*, *op. cit.*, p. 21 : En affirmant dans sa décision du 25 janvier 1985 concernant la loi relative à l'état d'urgence en Nouvelle Calédonie et dépendances (C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.*) que sans « la sauvegarde de l'ordre public […] l'exercice des libertés publiques ne saurait être assuré », le juge constitutionnel a reconnu un même niveau d'exigence à la liberté et à la sauvegarde de l'ordre public.

[1450] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, p. 1.

[1451] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 362 : Les mesures de police doivent donc « concilier, de la meilleure façon, l'ordre et la liberté, pour que celle-ci s'exerce grâce au respect de celui-là ».

[1452] DDHC, art. 4 : « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits » et DDHC, art. 5 : « La loi n'a le droit de défendre que les actions nuisibles à la société. Tout ce qui n'est pas défendu par la loi ne peut être empêché, et nul ne peut être contraint à faire ce qu'elle n'ordonne pas ».

limiter l'exercice[1453]. Le texte de la DDHC définit la liberté « par rapport à autrui »[1454] ; en d'autres termes il décrit une liberté propre à l'individu. À l'inverse, l'ordre public se définit par rapport au collectif, à la société et vient par conséquent limiter tout acte qui nuirait à son existence. L'existence de l'ordre public et des libertés repose par conséquent sur un équilibre fragile traduit par une tension permanente propre à l'exercice des droits et libertés.

542. Ainsi, la liberté[1455] et l'ordre public, bien que parfaitement opposés, ne peuvent exister l'un sans l'autre. Ils constituent un rapport « essentiel » au fonctionnement d'un État qui doit en assurer l'équilibre. L'ordre public comprend des éléments qui visent tant à protéger les droits et libertés qu'à restreindre ces mêmes droits et libertés[1456]. Ces dernières années, c'est au nom de l'ordre public, ou plus précisément à celui de la sécurité intérieure, que le législateur a adopté de nombreuses lois restreignant considérablement les droits et libertés[1457]. Le professeur Etienne Picard s'était demandé sur quels textes le législateur se reposait afin d'imposer des restrictions à des libertés ou à des droits constitutionnels en vue de préserver l'ordre public[1458]. Afin d'y répondre, il avait émis l'hypothèse que « dans la mesure où les droits affectés ont valeur constitutionnelle »[1459] ce pouvoir du législateur serait également d'origine constitutionnelle. En ce sens, il rappelait que certaines dispositions constitutionnelles, énonçant un droit ou une liberté, comprenaient une réserve expresse d'ordre public. Toutefois, il constatait que l'énoncé des normes constitutionnelles consacrant des droits ou libertés ne mentionnait aucune dérogation particulière à leur application. Il en avait alors conclu qu'il existait une norme constitutionnelle implicite autorisant le législateur à

[1453] Le vice-président du Conseil d'État soulignait ainsi que « les jurisprudences constitutionnelle et européenne reconnaissaient […] que la sauvegarde de l'ordre public, objectif de valeur constitutionnelle ou motif légitime prévu par la loi dans une société démocratique, autorise les restrictions ponctuelles à certaines libertés, en particulier afin de préserver leur effectivité globale » (SAUVÉE (J-M.), « Introduction », *in L'ordre public, regards croisés du Conseil d'État et de la Cour de cassation*, Colloque du 24 février 2017).

[1454] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, p. 1.

[1455] Entendu comme l'ensemble des droits et libertés constitutionnellement garantis, au premier rang desquels se trouve la sûreté.

[1456] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, p. 9 : Le rôle de l'ordre public « consiste à justifier des restrictions aux droits et libertés afin d'assurer les conditions sociales de leur exercice ».

[1457] Voir Annexe 3.

[1458] PICARD (E.) « Introduction générale », pp. 17-61, p. 19 *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public oui ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 28.

[1459] *Ibid.*

limiter les droits et libertés au motif de l'ordre public[1460].

543. Ainsi, depuis de nombreuses années, le juge constitutionnel s'assure que le texte de loi soumis à son contrôle de constitutionnalité opère une conciliation entre la nécessité du droit ou de la liberté constitutionnellement garantie, d'une part, et la préservation de l'exigence de sauvegarde de l'ordre public, d'autre part[1461]. Cet exercice de conciliation du Conseil constitutionnel se retrouve dans de nombreuses décisions[1462] dont celles reposant notamment sur l'examen des dispositions législatives relatives aux dispositifs de vidéoprotection y compris « augmentés »[1463]. Si le rapport entre l'ordre public et les libertés (qui inclut la sûreté individuelle) permettent d'assurer un équilibre nécessaire au maintien de l'État de droit, l'introduction de la sécurité en substitution de la sûreté bouleverse cet équilibre par la volonté du législateur d'en faire « la première des libertés »[1464], qui mêlerait les deux notions en perpétuelle opposition d'ordre public et de sûreté.

B. La substitution de la sûreté par la sécurité comme facteur de déséquilibre de l'État de droit

544. La substitution progressive du terme de « sûreté » par celui de « sécurité » vient modifier le contenu de l'obligation d'agir qui pèse sur l'État pour assurer les droits et libertés (1). Loin de se limiter à un glissement sémantique, les autorités publiques ont progressivement instauré une politique œuvrant en faveur d'une augmentation de la sécurité en faveur d'une meilleure répression et prévention des infractions au moyen de technologies destinées à la surveillance de la voie publique (2).

[1460] *Idem*, p. 29.

[1461] FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, *op. cit.*, p. 579. Voir aussi : BURG (M.), *Droit fondamental et opérationnel du maintien de l'ordre public*, *op. cit.*, p. 27 : « Si la notion d'ordre public connaît un champ d'application assez vaste au plan constitutionnel, elle n'en demeure pas moins encadrée par les conciliations qu'elle doit opérer avec les autres valeurs constitutionnelles dégagées par le Conseil ».

[1462] Voir notamment : C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.*, cons. 8 ; C. const., Décision n° 2005-532 DC, 19 janvier 2006, *op. cit.*, cons. 9 ; C. const., Décision n° 2010-613 DC, 7 octobre 2010, *Loi interdisant la dissimulation du visage dans l'espace public*, Rec. p. 276, cons. 5 [en ligne] ; C. const., Décision n° 2011-625 DC, 10 mars 2011, *op. cit.*, cons. 50 ; C. const., Décision n° 2015-478 QPC, 24 juillet 2015, *Association French Data Network et autres*, *JORF* n°0171 du 26 juillet 2015 page 12798, n° 42, cons. 16 [en ligne].

[1463] C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 16 (caméras fixes) ; C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 5 (caméras aéroportées) ; C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.*, cons. 32 (caméras fixes et aéroportées « augmentées » à des fins expérimentales).

[1464] CSI, art. L. 111-1.

1. Le paradigme de la prédominance de la sécurité sur la sûreté

545. La formule de Nicolas Boileau selon laquelle « ce que l'on conçoit bien s'énonce clairement, et les mots pour le dire arrivent aisément »[1465] semble être largement tenue en échec par l'introduction du concept de « sécurité ». La substitution fréquente du terme de sûreté par celui de sécurité dans les textes juridiques et dans les discours politiques en est le parfait exemple. Si l'emploi du terme de sécurité parait anodin, son introduction met pourtant à mal l'équilibre institué par le rapport entre libertés et ordre public en ayant recours à un terme aux sens multiples[1466]. Le fait est qu'à l'inverse de l'ordre public, le concept de sécurité répond à une demande sociale[1467]. En ce sens, le professeur Bertrand Warusfel déclarait qu' « à côté d'un sens traditionnel apparu dès la Renaissance, la sécurité a pris aujourd'hui une signification moderne qui en fait une demande sociale et politique majeure dans les sociétés développées »[1468]. Dans le même sens, le Professeur Didier Truchet affirmait que « le thème de la sécurité ne cess[ait] de s'enrichir pour répondre à la demande sociale » au point qu' « aujourd'hui tout se passe comme si une obligation de sécurité non exclusive mais générale pesait sur l'État »[1469].

546. L'introduction du concept de sécurité dans la législation et la doctrine peut effectivement surprendre puisqu'à la lecture de la Constitution de 1958 le texte ne fait aucune mention du terme « sécurité »[1470]. Depuis les premières Constitutions françaises, les constituants préfèrent le terme de

---

[1465] BOILEAU (N.), *L'Art poétique*, 1872, Volume 1, Chant I, pp. 203-211.

[1466] En ce sens, la professeure Christine Lazerges affirme « qu'il n'y a pas une sécurité mais des sécurités, car la vie nous confronte à de multiples insécurités » (LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.*). Voir aussi : VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 91 : « la sécurité fait l'objet de nombreuses déclinaisons, qui ne permettent pas vraiment de la saisir dans son intégralité » ; DELVOLVÉ (P.), « Sécurité et sûreté », *op. cit.*

[1467] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 346 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 234 ; DURAND (F.), « La notion de sécurité intérieure à travers les livres blancs et le code de la sécurité intérieure », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, p. 252 ; GLEIZAL (J-J.), « La sécurité : une nouvelle politique », *RFAP* n° 91, 1999, p. 369.

[1468] WARUSFEL (B.), « Les notions de défense et de sécurité en droit français », *Droit & Défense* 94/4, octobre 1994, p. 11. Voir aussi : GLEIZAL (J-J), *La police en France*, Paris, PUF, coll. Que sais-je ?, n° 2761, 1993, 128 p., p. 69 : « sous l'empire traditionnel de l'ordre public, l'ordre était défini par le haut, il l'est désormais, à l'ère de la sécurité, en fonction d'une demande sociale ».

[1469] TRUCHET (D.), *Le droit public*, Paris, PUF, coll. Que Sais-je ?, 2018, 128 p., p. 62.

[1470] GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 du droit de la sécurité et de la défense*, op. cit., pp. 19-29, spéc. p. 20 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 234.

sûreté (institutionnelle) à celui de sécurité[1471]. L'emploi du terme sécurité en droit constitutionnel est somme toute assez récent puisqu'il n'est apparu pour la première fois que dans la Constitution de 1946[1472]. Cependant, la Constitution de 1958 est revenue à cette constance des textes constitutionnels qui exclue le terme de sécurité, à l'exception des références faites à la sécurité sociale[1473], et se limite à des notions s'en approchant[1474]. La sécurité serait ainsi présente mais uniquement de manière implicite au sein des textes constitutionnels. Si l'introduction du terme de sécurité dans les discours et textes législatifs demeure assez « nouvelle », la banalisation de son emploi - surtout lorsqu'il se substitue à celui de sûreté - révèle « un changement de paradigme »[1475].

547. La formule politique, inlassablement répétée depuis la loi du 2 février 1981[1476], dite « Sécurité et liberté » ou « loi Peyrefitte »[1477], selon laquelle « la sécurité est la première des libertés » est à l'origine de la substitution fréquente du terme de sûreté par celui de sécurité dans les textes juridiques et dans les discours politiques. Cette loi traduit tant l'objectif sécuritaire du pouvoir politique[1478] que la volonté de transformer l'emploi terminologique du sujet opposant les libertés à l'ordre public. Toutefois, ce sont principalement les attentats du 11 septembre 2001 qui ont permis de parachever ce basculement vers un objectif sécuritaire privilégiant la sécurité sur la sûreté[1479] reposant « sur l'illusion d'une vie sans dangers » et qui a permis de « légitimer l'intrusion dans les libertés individuelles »[1480]. Pourtant, il convient de rappeler que la sécurité ne doit pas être

---

[1471] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 79 : Les Constitutions de 1791 à 1946 préfèrent le terme de sûreté publique ou nationale à celui de sécurité à l'exception, toutefois, de la Constitution de 1848 qui mentionnait, en son article 8, les termes de « sécurité publique » comme limite au droit d'association, de réunion, de pétition et d'expression. Voir aussi : LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme », *op. cit.*, spéc. p. 612.

[1472] Préambule de la Constitution de 1946, alinéa 11 (relatif à la sécurité matérielle) et alinéa 17 (réactif à la sécurité et au bien-être des nations et des peuples composant l'Union française).

[1473] Constitution française de 1958, art. 34, 39, 47-1 et 47-2.

[1474] *Idem*, notamment art. 5 (fonctionnement des pouvoirs publics), art. 16 (régimes exceptionnels de police), art. 34 (défense nationale).

[1475] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 84.

[1476] Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes, *op. cit.*

[1477] Du nom de son rédacteur principal Alain Peyrfitte (ministre de la Justice, garde des sceaux, ayant soutenu le projet de loi « Sécurité et liberté ») qui avait déclaré lors des débats à l'Assemblée nationale que : « Liberté et sécurité sont solidaires. La sécurité est la première des libertés ; inversement, il n'y pas de liberté sans une sécurité qui garantisse qu'on pourra en jouir » (AN, Compte-rendu intégral, 2ème séance, 11 juin 1980, *JO* Déb. AN 1980, p. 1749 [en ligne]).

[1478] PERERA (S.), *Le principe de liberté en droit public français*, *op. cit.*, p. 220.

[1479] Voir en ce sens : LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *op. cit.*, p. 9.

[1480] DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, p. 23.

confondue avec le droit à la sûreté, aujourd'hui appelée liberté individuelle, dont les fondements sont établis par la DDHC (pour le droit à la sûreté) et par la Constitution de 1958 (pour la liberté individuelle)[1481]. De fait, le fondement de la sécurité n'est pas explicitement établi par la Constitution française hormis par son rattachement en tant qu'élément de l'ordre public[1482].

548. Afin de maintenir le contrat social sur lequel se fonde la société, l'État doit remplir un devoir en matière de sécurité[1483]. En d'autres termes, l'autorité de police a le devoir de mettre en œuvre des mesures juridiques et matérielles afin de prévenir les menaces à l'ordre public dont elle a connaissance[1484]. Le constat, depuis les années 1980, d'une augmentation de la délinquance et d'une demande croissante de sécurité en France a incité les forces publiques à faire usage des premières caméras filmant la voie publique dans les années 1990 comme moyen de lutte contre les infractions (v. **n° 92 et suiv.**). La propagation du sentiment d'insécurité dans le monde entier suite aux attaques terroristes survenues depuis le début des années 2000 n'a fait qu'accroître le recours aux technologies de surveillance comme moyen de remplir les obligations de sécurité dues par l'État[1485]. Ces constats ont conduit à ce que cette obligation de sécurité ne se limite plus simplement à la répression des infractions mais aussi à la prévention de leur survenance ; ce que le professeur Maurice Cusson qualifiera « d'obligation de prévoyance »[1486].

[1481] Voir notamment : LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *op. cit.*, p. 8 ; GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* ; BEAUSSONIE (G.), « Le nouvel antagonisme entre sécurité et sûreté (à propos de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme) », *Revue de jurisprudence commerciale* n° 1, janvier/février 2018 ; LAZERGES (C.), « Le droit à la sécurité a-t-il effacé le droit à la sûreté ? L'exemple de la loi « Sécurité globale » », *op. cit.*

[1482] Voir notamment : C. const., Décision n° 80-127 DC, 20 janvier 1981, *op. cit.*, cons. 55 et 56 ; C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*, cons. 2 et 16.

[1483] CSI, art. L. 111-1 : « L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens ». Voir en ce sens : TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, pp. 299-316 ; GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 193 ; TRUCHET (D.), *Le droit public*, p. 63 ; VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 85 ; DOARÉ (R.) et FRUSTIÉ (M.), *Droit de la sécurité intérieure*, Paris, Lextenso, 2019, 171 p., pp. 108-109.

[1484] TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 301.

[1485] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, pp. 191 et suiv.

[1486] CUSSON (M.), « La surveillance et la télésurveillance : sont-elles efficaces ? », *Revue internationale de criminologie de police technique et scientifique* n° 2, 2005, p. 132.

549. La réaffirmation de la légitimité du pouvoir régalien a pris forme sous les traits de nouvelles dispositions législatives visant à prévenir les infractions. Le législateur a donc progressivement introduit de nouvelles lois en matière de police permettant la sauvegarde de l'ordre public ou la recherche des auteurs d'infractions par des moyens policiers visant à prévenir la commission d'infractions dans un cadre de police administrative. Ces textes visent principalement à prévenir les atteintes portées à la sécurité des personnes et des biens dans les lieux où sont susceptibles de survenir des infractions. Au sein de cette législation, la vidéoprotection reflète l'exemple le plus emblématique des mesures de police préventive qui, comme l'affirme Marc-Antoine Granger, « est devenue un maillon essentiel de la politique de sécurité intérieure »[1487]. En ce sens, il suffit d'observer l'évolution croissante de son cadre législatif[1488] pour constater l'ampleur de l'emprise de cette technologie et de ses conséquences sur les activités policières[1489].

2. Les raisons d'une politique sécuritaire

550. Certains auteurs ont avancé des arguments expliquant ce renouvellement de la politique en matière de sécurité publique. Ainsi, Francis Lamy, ancien préfet de région, avançait le fait que les enjeux de sécurité publique diffèrent selon les types de territoires et appellent des modes opératoires distincts. Aussi, il formulait le constat « d'une extension des zones périurbaines » ayant pour conséquence d'importer en zones rurales des « formes de délinquances urbaines - trafics de stupéfiants, incivilités, petite délinquance de voie publique - » nécessitant une adaptation des modes opératoires des forces de l'ordre dans ces zones[1490]. À titre d'exemple, la périphérie de Lyon[1491] s'était précisément trouvée dans cette situation où pour faire face à cette délinquance les forces de

---

[1487] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 193.

[1488] Voir principalement : Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), *op. cit.* ; Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), *op. cit.* ; Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *op. cit.* ; Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure (RPSI), *op. cit.* ; Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.*

[1489] Voir notamment : LATOUR (X.), « Sécurité intérieure : un droit "augmenté" », *op. cit.* ; HANICOTTE (R.), « Espace public, impasse des libertés », *op. cit.*

[1490] LAMY (F.), « La production de la sécurité publique », pp. 17-34, spéc. p. 20 *in* SÈVE (R.), *L'ordre public*, *op. cit.*

[1491] Témoignage de la police nationale de Lyon AN2V lors du Webinar organisé en partenariat avec l'AN2V, « Caméras-piétons : quels bénéfices pour les forces de Police et la population ? », *Axis Communication*, 24 septembre 2020 [en ligne].

l'ordre avaient eu pour la première fois recours à des caméras individuelles (ou caméras piétons)[1492] leur permettant de filmer et de collecter des éléments de preuve lors de leurs interventions.

551. Un autre argument serait l'évolution naturelle des attentes de la société en matière de sécurité publique. La préservation de l'ordre public comprend différents types d'actions dont celles visant à prévenir les infractions. De manière complémentaire aux actions de répression (action de réaction) de la part des forces de l'ordre à la commission d'une infraction, les actions de prévention reposent sur une anticipation de celles-ci. À cette fin, la mise en œuvre de caméras filmant la voie publique est progressivement apparue aux yeux des forces de l'ordre comme un outil nécessaire, voire indispensable à l'exécution des missions de prévention des infractions relevant du cadre de la police administrative[1493].

552. Conclusion - Force est de constater que les technologies numériques contribuent insidieusement au renforcement des dispositions relatives à la sécurité au regard de leur multiplication au sein de la législation en dépit de la position qu'occupe la sécurité au sein de la hiérarchie des normes (objectif de valeur constitutionnelle) par rapport à des droits et libertés élevés au rang de principes fondamentaux constitutionnels. La prédominance de la sécurité sur la sûreté se révèle principalement au travers des dispositions de prévention des infractions. Celles-ci participent à l'amenuisement de la sûreté qui, à l'origine, reflétait la volonté des constituants de protéger les individus contre une suspicion arbitraire et générale de l'État. Or, le recours croissant aux outils technologiques par les forces de l'ordre ne fait qu'amplifier l'effet de suspicion généralisée de la population. La multiplication et la diversité des systèmes de surveillance à l'usage de la sécurité publique semblent inverser le principe de la présomption d'innocence pour tendre vers une présomption de culpabilité des individus observés sous réserve de ne pas commettre d'infraction. Les drones aériens « augmentés » de sécurité publique, bien qu'ayant vocation à être utilisés de manière limitée dans le temps et dans l'espace, participent au phénomène favorisant la « sécurité »

[1492] Les caméras individuelles sont placées sur les uniformes des agents lors des missions et permettent de filmer les évènements lors d'une intervention. Elles sont portées par les agents de manière visible et doivent être signalées aux personnes concernées avant le commencement de l'enregistrement. Les images peuvent désormais être transmises en direct au poste de commandement. Elles ont fait l'objet d'un premier encadrement par une loi du 3 juin 2016 [Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale, *op. cit.*] puis par la loi relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique [Loi n° 2018-697 du 3 août 2018 relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique, *JORF* n°0179 du 5 août 2018, [en ligne]] et enfin, plus récemment, par la loi RPSI [Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, *op. cit.*].

[1493] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 193.

du collectif sur la sûreté des individus. Aussi, la multiplication des technologies de surveillance de sécurité publique, principalement en matière de prévention des incidents et des infractions par le traitement et l'analyse de données, participent à la « promotion » de la sécurité qui tente de s'élever au rang de droit constitutionnel voire de droit « fondamental ».

Section 2 L'aggravation du bouleversement dans le rapport sûreté-sécurité à l'ère des technologies de surveillance de la voie publique

553. Le premier article du CSI énonçant que « la sécurité est un droit fondamental et l'une des conditions d'exercices des libertés individuelles et collectives »[1494] laisse les juristes pour le moins pantois[1495]. Cette formulation n'est pourtant pas inédite puisqu'elle reprend, en partie, celle énoncée par la loi n° 95-73 du 21 janvier 1995, dite LOPS[1496]. Aujourd'hui, la sécurité fait toujours débat en doctrine quant à sa qualification même de droit[1497] qui préserverait dans le même temps l'ordre public et les libertés individuelles[1498] bien qu'il permette de les limiter. Plusieurs auteurs ont même tenté de déterminer si la sécurité revêtait non pas seulement la qualification de droit mais également celle d'un droit fondamental[1499]. À l'heure où les technologies de surveillance semblent avoir pris une place prépondérante au sein de l'arsenal policier, il paraît opportun de chercher à déterminer si l'accroissement de leur mise en œuvre résulte de l'existence d'un droit à la sécurité et d'étudier l'éventualité de sa qualité de droit fondamental (§1).

[1494] CSI, art. L. 111-1.

[1495] LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *op. cit.* ; CHAMPEIL-DESPLATS (V.), « Les enjeux normatifs de la fondamentalisation du droit à la sécurité », p. 81 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.* ; VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? » p. 98 *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.* ; DUPRÉ DE BOULOIS (X.), « Existe-t-il un droit fondamental à la sécurité ? », p. 197 *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.* ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.* , p. 345.

[1496] Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), *op. cit.*, art. 1er.

[1497] Voir notamment : NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.* ; AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, Paris, LGDJ Éditions Institut Universitaire Varenne, coll. « Colloques & Essais », 2019, 232 p. ; LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *op. cit.*

[1498] MAUBERNARD (C.), « Vers une fondamentalisation du droit à la sécurité ? », *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 173-187, p. 176 : « Le droit à la sécurité a en effet une dimension tant individuelle que collective, transcendantale en ce sens qu'il ne serait ni possible ni même souhaitable de distinguer les deux dimensions ».

[1499] Voir notamment : TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.* ; GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* ; CAUSSE (H.), « Le principe de sûreté et le droit à la sécurité », *Gaz. Pal.* n°354, 20 décembre 2001, pp. 2-6.

554. Au-delà des questions concernant la « fondamentalisation » d'un droit à la sécurité, le recours exponentiel aux technologies de surveillance de la voie publique par les forces de l'ordre questionne l'encadrement de leurs usages définis par la distinction opposant la police administrative à la police judiciaire, atténuée par le basculement des missions du caractère préventif à celui de répressif. Aussi, l'introduction des drones aériens de sécurité publique pourrait amplifier ce phénomène. En outre, l'emploi de technologies de surveillance « augmentées » filmant la voie publique soulève des enjeux de légitimité tant au regard de la nécessité de leur emploi par les forces de l'ordre qu'au regard des risques que leur recours est susceptible d'engendrer sur les DACP des personnes observées (§2).

§1. Les technologies de surveillance de sécurité publique supports d'une fondamentalisation d'un droit à la sécurité

555. Si l'existence d'un devoir de l'État de mettre en œuvre les mesures adaptées afin de prévenir les atteintes à l'ordre public n'est plus sujette au débat, la question demeure de savoir si cette obligation induit nécessairement un droit à la sécurité à l'égard des personnes, justifiant la prolifération des usages des caméras filmant l'espace public (A). Nonobstant le fait que la doctrine demeure divisée sur la qualification de la sécurité en tant que droit, le législateur n'a pas attendu qu'il y ait un consensus pour attribuer à la sécurité le caractère de droit fondamental, amplifiant ainsi encore le débat (B).

A. La détermination d'un droit à la sécurité au travers des technologies de surveillance de sécurité publique

556. « La sécurité est la première des libertés » énonçait Alain Peyrefitte lors de l'élaboration de la loi dite « Sécurité et liberté » de 1981[1500]. Cette formule, mainte fois répétée, a été réaffirmée à trois reprises par le législateur[1501]. Il est vrai que la sécurité est souvent présentée comme étant la

[1500] Loi n° 81-82 du 2 février 1981 renforçant la sécurité et protégeant la liberté des personnes, *op. cit.*

[1501] Loi n° 95-73 du 21 janvier 1995 (LOPS), *op. cit.*, art. 1er : « la sécurité est un droit fondamental et l'une des conditions d'exercice des libertés individuelles et collectives » ; Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *op. cit.*, art. 1er : « La sécurité est un droit fondamental. Elle est une condition de l'exercice des libertés et de la réduction des inégalités » ; Loi n° 2003-239 du 18 mars 2003, *op. cit.*

première mission régalienne de l'État[1502] mais avant d'entreprendre une recherche de l'existence d'un droit à la sécurité, il convient de préciser le sens qui est ici attribué au terme de « sécurité ». L'introduction de cette étude a permis de mettre en lumière la multiplicité des sens que peut prendre la « sécurité » (v. **n° 53 et suiv.**). Elle peut notamment faire référence au « sentiment d'insécurité » exprimé par les citoyens et décrit dans le rapport Peyrefitte[1503]. Toutefois, comme l'affirme à juste titre Marc-Antoine Granger, cette vision de la sécurité s'inscrit davantage dans une dimension sociologique que juridique[1504]. Dès lors, il convient d'attribuer au terme de « sécurité » un sens objectif tel que la protection des personnes et des biens résultant d'une menace à leur encontre[1505]. Dans une première hypothèse, la recherche d'un droit à la sécurité peut se trouver dans l'obligation qui incombe aux États d'adopter des mesures préservant l'ordre public (1). Dans, une deuxième hypothèse, la sécurité tente de s'ériger en droit sous l'influence d'une politique sécuritaire adoptant les exigences propres au principe de précaution avant de se diriger vers le concept de « dangerosité » (2).

1. Un droit à la sécurité fondé sur l'obligation d'agir des États

557. L'existence d'un droit à la sécurité pourrait se trouver dans le lien qui l'unit à l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public[1506] qui inclut la sécurité des personnes et des biens[1507] ; en d'autres termes, au devoir de l'État d'assurer la sécurité sur son territoire[1508]. Cette

---

[1502] Voir notamment : GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* ; VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 86.

[1503] Rapport dit Peyrefitte à M. le président de la République présenté par le comité d'études sur la violence, la criminalité et la délinquance, 27 juill. 1977, *La documentation française*, 193 p., p. 34 [en ligne] : « Dans la France d'aujourd'hui, une peur enfouie au plus profond de l'homme, mais effacée pour un temps des mémoires, est réapparue sous la forme d'un sentiment d'insécurité » et d'ajouter que « la résurgence de cette vieille crainte est un phénomène cyclique ».

[1504] GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.*

[1505] La menace fait référence au caractère intentionnel de l'atteinte portée à l'intégrité d'un individu ou à un bien à l'inverse d'un danger qui exclu cette intention (ex. catastrophe naturelle). Voir sur cette différence : Ministère de la Défense, Livre Blanc « Défense et Sécurité nationale », juin 2008, 760 p., p. 386 [en ligne].

[1506] DUPRÉ DE BOULOIS (X.), « Existe-t-il un droit fondamental à la sécurité ? », *RDLF*, 2018, chron. 13 [en ligne].

[1507] C. const., Décision n° 80-127 DC, 20 janvier 1981, *op. cit.*

[1508] C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.* : Dans sa décision, le Conseil constitutionnel confère à l'ordre public le caractère d'objectif de valeur constitutionnelle sur le fondement de l'article 34 de la Constitution de 1958 (LARRALDE (J-M.), « La constitutionnalisation de l'ordre public », *in* REDOR (M-J.) (dir.), *L'ordre public : ordre public ou ordres publics ? Ordre public et droits fondamentaux*, op. cit., p. 226). C'est également ce qu'énonce l'article 1er de la LOOPSI : « l'État a le devoir d'assurer la sécurité en veillant sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre public, à la protection des personnes et des biens ».

obligation de l'État se traduit également dans la jurisprudence du Conseil d'État[1509] qui énonce de manière constante que « l'autorité de police est tenue de prendre les mesures adéquates pour prévenir les risques de troubles pour l'ordre public dont elle a connaissance »[1510]. En ce sens, seule l'autorité de police serait en charge d'assurer des obligations de sauvegarde de l'ordre public et engagerait sa responsabilité en cas d'inaction en connaissance d'évènements ayant troublé l'ordre public. Bien qu'un tel droit à la sécurité ne soit nullement inscrit au sein de la Conv.EDH européenne des droits de l'homme[1511], le juge européen des droits de l'Homme reconnaît que la responsabilité de l'État peut être engagée lorsque des « circonstances spécifiques ont entrainé une atteinte à la sécurité des individus »[1512]. C'est sur le fondement du droit à la vie, énoncé à l'article 2 de la Conv.EDH[1513], que la CEDH a développé cette obligation positive opposable à l'État qui doit « prendre les mesures nécessaires à la protection de la vie des personnes relevant de sa juridiction »[1514]. Ainsi, elle a affirmé à plusieurs reprises que l'État « a le devoir primordial d'assurer le droit à la vie en mettant en place une législation pénale concrète dissuadant de commettre des atteintes contre la personne et s'appuyant sur un mécanisme d'application conçu pour en prévenir, réprimer et sanctionner les violations »[1515]. En conséquence, le droit à la vie peut engendrer des obligations positives à l'égard de l'État pouvant aller jusqu'à l'adoption de mesures préventives nécessaires[1516] telles qu'à des fins de lutte contre le terrorisme.

558. Pour autant, affirmer que l'État serait débiteur d'un « droit à la sécurité » parait peu réaliste tant il s'avère impossible de prévenir toutes les atteintes portées à l'intégrité des

---

[1509] CE, 23 octobre 1959, n° 40922, *Doublet* et CE, 14 décembre 1962, *Doublet*, Rec. p. 680 [en ligne].

[1510] TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 299.

[1511] AFROUKH (M.), « L'émergence d'un droit à la sécurité dans la jurisprudence de la Cour européenne des droits de l'homme », *RDP* n°1, 2015, p. 139 ; AFROUKH (M.), « Existe-t-il un droit fondamental à la sécurité dans le cadre de la Convention européenne des droits de l'homme ? », in AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 209-220, spéc. p. 210.

[1512] MAUBERNARD (C.), « Vers une fondamentalisation du droit à la sécurité ? », *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 173-187, p. 178.

[1513] Conv.EDH, art 2, §1 : « Le droit de toute personne à la vie est protégé par la loi ».

[1514] CEDH, 9 juin 1998, *L.C.B. c. Royaume-Uni*, n° 14/1997/798/1001, §36 [en ligne].

[1515] Voir notamment : CEDH, 28 octobre 1998, *Osman c. Royaume-Uni*, n° 87/1997/871/1083, § 115 [en ligne] ; CEDH 28 mars 2000, *Kiliç c. Turquie*, n° 22492/93, §62 [en ligne] ; CEDH, 14 juin 2011, *Ciechońska c. Pologne*, n° 19776/04, §48 [en ligne].

[1516] GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.*

individus[1517]. En ce sens, le Conseil d'État, tout en réaffirmant l'obligation de l'État d'assurer la sécurité publique, a clairement énoncé dans un arrêt du 20 juillet 2001 que « la méconnaissance de cette obligation ne constitu[ait] pas par elle-même une atteinte grave à la liberté fondamentale »[1518]. De même, la CEDH reconnait que ce devoir de l'État ne peut lui imposer « un fardeau insupportable ou excessif » et que « toute menace présumée contre la vie n'oblige pas les autorités, au regard de la Convention, à prendre des mesures concrètes pour en prévenir la réalisation »[1519]. Dès lors, cette exigence à l'égard des pouvoirs publics ne peut relever que d'une obligation de moyens pouvant donner lieu à des sanctions en cas de manquement[1520]. L'existence d'un droit à la sécurité relèverait donc davantage de la volonté du législateur que de celle des juridictions nationales[1521].

2. Un droit à la sécurité « justifié » par l'exigence d'anticipation des atteintes aux personnes et aux biens

559. Le principe de précaution, support d'un droit à la sécurité - Les évolutions juridiques en matière de sauvegarde de l'ordre public ont fait apparaitre de nouvelles exigences préalables à l'obligation d'agir. Désormais, les pouvoirs publics n'ont plus seulement pour obligation de réagir aux risques d'atteintes portées à l'ordre public et sont aussi tenus de rechercher et d'identifier les risques potentiels pour l'ordre public[1522]. La liste des finalités permettant le recours à des dispositifs de vidéoprotection[1523] sont une illustration de cette obligation d'identification des risques pouvant porter atteinte à l'ordre public. Ce sont les exigences croissantes de sécurité, formulées par la

---

[1517] *Idem*, p. 303 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 345. Voir aussi en ce sens : DE MONTALIVET (P.), « Les objectifs de valeur constitutionnelle », *Cahiers du Conseil constitutionnel* n° 20, juin 2006 [en ligne] : « Les objectifs ne constituent pas des obligations de résultat, dans la mesure où ils n'obligent pas le législateur quant à un résultat précis et où leur mise en œuvre aboutit à un résultat aléatoire. La fonction d'obligation des objectifs est ainsi limitée ».

[1518] CE, ord., 20 juillet 2001, *Commune Mandelieu-la-Napoule*, n° 236196 [en ligne].

[1519] Voir en ce sens : CEDH, 28 octobre 1998, *Osman c. Royaume-Uni*, *op. cit.*, § 116 ; CEDH, 28 mars 2000, *Mahmut Kaya c. Turquie*, n° 22535/93, §86 [en ligne].

[1520] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, pp. 345-346.

[1521] MAUBERNARD (C.), « Vers une fondamentalisation du droit à la sécurité ? », *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 173-187, p. 179.

[1522] TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 302 ; DUPRÉ DE BOULOIS (X.), « Existe-t-il un droit fondamental à la sécurité ? », *op. cit.* : « il ne s'agit plus seulement d'assurer *a posteriori* la réparation et la sanction des manquements ou des atteintes à la sécurité des personnes mais de prévenir en amont la survenance de ce type d'atteintes ».

[1523] CSI, art. L. 251-2 (caméras fixes) et art. L. 242-5 (caméras aéroportées).

population, qui ont conduit à l'extension du périmètre de cette obligation préalable d'identification des risques pour l'ordre public[1524]. Les exigences d'anticipation d'évènements à risque évoluent à mesure que le sentiment d'insécurité s'installe. Dès lors, les pouvoirs publics seraient tenus de chercher « le danger potentiel et ne plus attendre des certitudes raisonnables pour agir »[1525] en vertu de l'interprétation faite du principe de précaution par le législateur, qui exige de prendre toutes les mesures nécessaires en vue de prévenir les atteintes portées à la collectivité[1526]. De ce fait, le juge du référé-liberté peut désormais exiger de l'autorité publique de mettre en œuvre des mesures afin d'assurer la sécurité des personnes dès lors que « l'action ou la carence de l'autorité publique créé un danger caractérisé imminent pour la vie des personnes, portant ainsi une atteinte grave et manifestement illégale à cette liberté fondamentale, et que la situation permet de prendre utilement des mesures de sauvegarde dans un délai de quarante-huit heures »[1527].

560. Selon ce principe de précaution, les pouvoirs publics auraient pour obligation d'identifier et d'assurer le suivi des risques potentiels pour l'ordre public. Cette obligation instaure un devoir de vigilance tel qu'en matière de santé[1528]. À titre d'exemple, lors de la pandémie de COVID-19, l'État français avait ordonné par mesure de précaution sanitaire un confinement général de la population et appliqué le régime d'exception tenant à l'état d'urgence permettant la restriction de l'exercice de nombreux droits et libertés[1529]. Si l'apparition d'un grave trouble à l'ordre public peut justifier la mise en œuvre de la responsabilité de l'État en cas de carence, il parait inconcevable de lui attribuer une obligation d'intervenir dans toutes circonstances pour rétablir l'ordre public, qui à défaut d'exécution engagerait sa responsabilité[1530]. Pour autant, l'État est tenu de mettre en œuvre les

---

[1524] GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* : « Il faut reconnaitre qu'un sentiment d'insécurité entretenu par la permanence des menaces, notamment terroristes, et l'intolérance de plus en plus forte des individus à l'endroit de ces menaces à leur sécurité, font peser sur le pouvoir une contrainte telle qu'il semble tenu de réagir, voire d'agir, pour anticiper une éventuelle atteinte à la collectivité ».

[1525] TRUCHET (D.), « L'obligation d'agir pour la protection de l'ordre public : la question d'un droit à la sécurité », *in* REDOR (M-J.) (dir.), *L'ordre public : Ordre public ou ordres publics ? - Ordre public et droits fondamentaux*, *op. cit.*, p. 303.

[1526] GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.*

[1527] Exemple : CE, sect., 16 novembre 2011, n° 353172, *Ville de Paris* [en ligne].

[1528] À titre d'exemple : Loi n° 98-535 du 1 juillet 1998 relative au renforcement de la veille sanitaire et du contrôle de la sécurité sanitaire des produits destinés à l'homme, *JORF* n°151 du 2 juillet 1998 [en ligne].

[1529] Voir les 11 lois votées durant la période de la crise sanitaire (« Onze lois pour répondre à la crise sanitaire adoptées entre mars 2020 et juillet 2022 », *Vie publique*, 2 août 2022 [en ligne]).

[1530] À titre d'exemple, le Conseil d'État avait déjà eu l'occasion d'affirmer que « la difficulté de prévoir la nature, la date, le lieu et les objectifs » de certains événements tels que des actes terroristes ne constituent pas une faute de nature à engager la responsabilité de l'État (CE, 10 février 1982, n° 16137, *Compagnie Air-Inter*, Rec. p. 743 [en ligne]).

moyens suffisants afin de prévenir les évènements susceptibles de causer de graves troubles à l'ordre public tels que des actes terroristes. À titre d'exemple, l'adoption de la loi JOP2024 autorisant l'emploi de caméras « augmentées » filmant la voie publique se justifie au regard des circonstances exceptionnelles des évènements prévus en France durant l'année 2024. En revanche, il convient de s'interroger sur la légitimité du recours à de telles technologies en dehors de tout cadre « exceptionnel » ainsi que sur sa reconnaissance en tant que moyen suffisant pour assurer la sécurité des personnes et des biens.

561. La « dangerosité », prétexte d'un droit à la sécurité - Outre le principe de précaution, qui repose sur la notion de risque, l'affirmation d'un droit à la sécurité tente de se justifier au travers du concept de dangerosité qui s'est imposé dans le droit pénal[1531] (v. **n° 492**) depuis la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales[1532]. Lors du contrôle de constitutionnalité de cette loi, le Conseil constitutionnel avait regardé ce concept de dangerosité visant à prévenir la récidive « dont le risque est élevé » comme un moyen de « garantir l'ordre public et la sécurité des personnes »[1533]. Néanmoins, il est regrettable que ni le législateur ni le juge constitutionnel n'ait apporté de définition de la « dangerosité ». Le concept est lui-même dangereux[1534] dans la mesure où il porte atteinte à l'État de droit par les droits et libertés qu'il restreint ainsi que par les discriminations qu'il peut engendrer[1535]. À l'heure où s'accroît le nombre des algorithmes destinés à un usage de sécurité publique, notamment ceux à des fins dites « prédictives »[1536], il est légitime de craindre que l'emploi de drones aériens « augmentés » de sécurité publique puisse aggraver ce phénomène qui tend à installer durablement le concept de dangerosité dans le droit commun pour justifier les besoins sociétaux de sécurité.

[1531] De manière non-exhaustive : DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, spéc. p. 467 ; ROUVILLOIS (F.), « La notion de dangerosité devant le Conseil constitutionnel », *Rec. Dalloz* 2006, 14, pp. 966-970 ; GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *op. cit.* ; LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.*

[1532] Loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales, *JORF* 13 décembre 2005, p. 19152 [en ligne].

[1533] C. const., Décision n° 2005-527 DC, 8 décembre 2005, *Loi relative au traitement de la récidive des infractions pénales*, Rec. p. 153, cons. 14 et 17 [en ligne].

[1534] Voir sur le sujet : LAZERGES (C.), « La dangerosité de la notion de dangerosité en droit pénal », *Criminocorpus* n° 20, 2022 [en ligne].

[1535] LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.*

[1536] *Ibid*.

562. Aujourd'hui, l'existence même d'un « droit à la sécurité » pose encore question et continue d'enrichir le débat au sein de la doctrine[1537]. Dès lors, affirmer l'existence d'un « droit à la sécurité » comme un droit individuel n'a que peu de sens. Ainsi, il apparait que l'existence du droit à la sécurité n'est qu'une illusion et que la consécration d'un tel droit ne soit ni utile ni même souhaitable[1538]. Aussi, dans le cas où un tel droit à la sécurité serait toutefois un jour explicitement reconnu, son caractère de droit fondamental semble être unanimement rejeté par la doctrine.

B. La fondamentalisation d'un droit à la sécurité au travers des technologies de surveillance de sécurité publique

563. Le premier article du CSI énonce que « la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives »[1539]. Pour autant, comme le rappelle à juste titre le professeur Olivier Gohin, cette affirmation « n'est pas, par elle-même, de droit constitutionnel comme il est nécessaire lorsqu'il s'agit d'apprécier la juste combinaison de l'exigence de sécurité publique et de la garantie des libertés fondamentales »[1540]. Afin de déterminer si la sécurité pourrait être un droit fondamental, il convient de définir au préalable ce qu'est un droit fondamental en s'appuyant principalement sur la jurisprudence du Conseil constitutionnel ainsi que celle des juridictions supranationales.

564. Origines du concept de « droit fondamental » - La qualification de droits et libertés fondamentaux n'est pas apparue avec les décisions du Conseil constitutionnel mais existe depuis un siècle au travers d'une ancienne doctrine qui défendait les droits fondamentaux de l'État[1541]. La notion de fondamentalité s'ancre véritablement lors de la rédaction de la « Loi fondamentale » de la République fédérale d'Allemagne adoptée le 23 mai 1949 qui énumère les différents « droits fondamentaux »[1542]. Le professeur Louis Favoreu fut l'un des premiers promoteur du concept de

---

1537 AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.* ; NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.* ; TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*

1538 DUPRÉ DE BOULOIS (X.), « Existe-t-il un droit fondamental à la sécurité ? », *op. cit.*

1539 CSI, art. L. 111-1.

1540 GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 du droit de la sécurité et de la défense*, op. cit., pp. 19-29, spéc. p. 24.

1541 POIRAT (F.), « La doctrine des « droits fondamentaux » de l'État », *Droits*, 1992, p. 83.

1542 CHAMPEIL-DESPLATS (V.), *Théorie générale des droits et libertés*, Paris, Dalloz, 2019, 452 p., p. 46 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 30.

« droit fondamental » en France qu'il qualifiait de « protection à un niveau supra-législatif (notamment constitutionnel) des droits et libertés »[1543]. Il avait défini le droit fondamental comme un « droit subjectif de valeur constitutionnelle ou conventionnelle qui s'accompagne d'un mécanisme de contrôle juridictionnel lui permettant de produire ses effets à l'encontre des normes inférieures »[1544]. De fait, un objectif de valeur constitutionnelle ne constitue qu'une simple finalité et ne peut donc être invoqué devant un juge à l'inverse d'un droit fondamental[1545].

565. L'inexistence d'un droit fondamental à la sécurité - Le juge constitutionnel ne reconnait pas le caractère de liberté ou de droit fondamental à l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public[1546]. De même, le Conseil constitutionnel ne reconnait pas le caractère de droit fondamental à la sécurité dans la mesure où dans sa décision du 13 mars 2003 portant sur la loi pour la sécurité intérieure[1547] il déclarait que lorsque « les dispositions contestées ne créent aucun droit nouveau au profit des personnes [et] qu'elles ne confèrent pas non plus à l'autorité administrative des pouvoirs dont elle ne disposerait pas déjà, elles sont […] dépourvues de caractère normatif ». De même, le Conseil d'État, lors de sa décision du 20 juillet 2001, avait refusé de reconnaitre au droit à la sécurité le caractère de liberté fondamentale au sens du référé-liberté[1548]. Toutefois, la constitutionnalisation de la sécurité s'opère de manière indirecte par le statut d'objectif de valeur constitutionnelle accordé à l'ordre public par le Conseil constitutionnel[1549] et dont elle constitue la composante principale[1550]. Aussi, l'utilisation alternative des termes de « sûreté » et de

---

[1543] FAVOREU (L.), *Droits des libertés fondamentales*, *op. cit.*, p. 70.

[1544] *Ibid*.

[1545] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 100.

[1546] C. const., Décision n° 2014-422 QPC, 17 octobre 2014, *Chambre syndicale des cochers chauffeurs CGT-taxis* [voitures de tourisme avec chauffeur], *JORF* n°0243 du 19 octobre 2014 page 17454 texte n° 44, cons. 12 [en ligne] : « l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public ne peut, en lui-même, être invoqué à l'appui d'une question prioritaire de constitutionnalité sur le fondement de l'article 61-1 de la Constitution ».

[1547] C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.*, cons. 90 [en ligne].

[1548] CE, ord., 20 juillet 2001, n° 236196, *op. cit.*

[1549] C. const., Décision n° 82-141 DC, 27 juillet 1982, *op. cit*. confirmée par C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.*, cons. 3 : « il appartient au législateur d'opérer la conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public sans lequel l'exercice des libertés ne saurait être assuré ».

[1550] GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 du droit de la sécurité et de la défense*, *op. cit.*, pp. 19-29, spéc. p. 25. Voir aussi : LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.* : « En droit interne, [le droit à la sécurité] est fondamentalisé par la loi française et implicitement par la jurisprudence du Conseil constitutionnel ».

« sécurité » par les politiques voudrait prêter à ce dernier un statut équivalent à celui du premier et ainsi bénéficier d'une valeur supra-législative.

566. En définitive, le « droit fondamental à la sécurité » n'a pas été consacré de manière explicite et ne dispose ainsi que d'une valeur législative[1551]. L'affirmation d'un droit fondamental à la sécurité est donc trompeuse et ne vise en réalité qu'à affirmer durablement une politique sécuritaire[1552]. Le fait est que la sécurité dispose d'un cadre juridique dense, notamment au travers des dispositions applicables en matière de vidéoprotection, en accord avec la volonté exprimée par les politiques à l'œuvre depuis une trentaine d'années. Cependant, cette politique sécuritaire entraine « une dérive législative, approuvée par l'opinion et qui, de lois en lois, ne cesse de faire reculer les mécanismes protecteurs de la sûreté individuelle »[1553].

567. Ainsi, la transformation de la sécurité en droit fondamental présente un danger pour les droits et libertés en « jouant un rôle invalidant, c'est à dire [en permettant] soit de censurer des dispositions législatives qui méconnaitraient ce droit à la sécurité, soit qui ne permettraient pas de l'assurer »[1554]. La multiplication des lois visant à amplifier les mesures en faveur de la sécurité intérieure associée au recours exponentiel à des dispositifs de surveillance de l'espace public participent à cette forme de fondamentalisation d'un « droit à la sécurité » dans la mesure où ils incarnent un des principaux outils de prévention à la commission des infractions et aux troubles à l'ordre public. Dès lors, les technologies de surveillance de sécurité publique s'intègrent dans cette politique sécuritaire. Aussi, en dépit des progrès technologiques et des opportunités que présentent les drones aériens de sécurité publique, il semble impossible de garantir la sécurité en tout temps au

---

[1551] CHAMPEIL-DESPLATS (V.), « Les enjeux normatifs de la fondamentalisation du droit à la sécurité », *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*, spéc. p. 101 ; MAUBERNARD (C.), « Vers une fondamentalisation du droit à la sécurité ? », *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 173-187, p. 179 ;

[1552] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 18 ; HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 346. Voir aussi : MAUBERNARD (C.), « Vers une fondamentalisation du droit à la sécurité ? », *in* AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, *op. cit.*, pp. 173-187, pp. 181-182 : « La fondamentalité a donc bien pour fonction ici de légitimer les moyens mis en œuvre par l'État, comme la novation du droit commun en droit dérogatoire » ; DUPRÉ DE BOULOIS (X.), « Des droits de l'homme au service de la puissance de l'État », *RDLF*, 2022, chron. 2 [en ligne].

[1553] LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *op. cit.*, p. 9. Dans le même sens, la professeure Christine Lazerges affirmait que « la fondamentalisation récente du droit à la sécurité entraîne de lourdes régressions du droit à la sûreté ou tout le moins un équilibre bien difficile à préserver entre le droit à la sûreté et le droit à la sécurité, le premier étant le noyau dur de l'État de droit » (LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.*).

[1554] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 101.

sein de l'espace public, qu'il s'agisse de prévenir toute atteinte à l'intégrité des personnes physiques ou tout autre trouble à l'ordre public. L'illusion que présente « le solutionnisme technologique » à des fins de sécurité publique tend à faire disparaitre les garanties juridiques face aux activités régaliennes qui reposent notamment sur les principes de nécessité et de proportionnalité. La multiplication des usages technologiques régaliens pourrait conduire à une perte de contrôle des pratiques des entités de l'État dont les conséquences peuvent être désastreuses pour les droits et libertés de chacun.

§2. Le recours aux technologies de surveillance « augmentées » de sécurité publique, support d'une redéfinition du rapport aux forces de l'ordre

568. L'introduction des technologies de surveillance à l'usage des forces de l'ordre, principalement les caméras, participe de longue date au phénomène de dissipation de la distinction entre la police administrative et la police judiciaire qui délimite les activités relatives à la prévention des infractions de celles de répression des atteintes portées à l'ordre public. Or, la dilution progressive de cette frontière entre police administrative et police judiciaire, loin d'être anodine, limite la protection des droits et libertés par une multiplication des mesures restrictives qui contournent le contrôle du juge judiciaire en adoptant un « profil » préventif. Le recours à des drones aériens, particulièrement ceux associés à des algorithmes d'analyse d'images, pourrait renforcer ce phénomène qui vise une recherche coercitive des infractions (A).

569. Les technologies de surveillance « augmentées » interrogent également la légitimité de leur usage à des fins de sécurité publique dans la mesure où il a été constaté que les forces de l'ordre disposent rarement d'un contrôle continu de leur développement et de leur fonctionnement, d'une part, et que la fiabilité de leurs résultats n'a pas encore été démontrée, d'autre part. En outre, le recours à ces technologies pourrait susciter des inquiétudes légitimes quant à leur nécessité et à leur proportionnalité à des fins de prévention des infractions, notamment si des données sensibles devaient faire l'objet d'un traitement à ces fins (B).

A. Un renforcement de l'atténuation de la distinction entre police administrative et police judiciaire

570. En France, il existe une distinction primordiale entre la police administrative et la police judiciaire. Elle est apparue dès la période révolutionnaire[1555] et se reflète au travers de la décision du Conseil constitutionnel du 23 janvier 1987 qui, se reposant sur l'article 34 de la Constitution, avait rappelé qu'il appartenait au législateur « de fixer les limites de la compétence des juridictions de l'ordre administratif et de l'ordre judiciaire »[1556]. Cette distinction entre police administrative et police judiciaire repose originellement sur un « principe de séparation des autorités administratives et judiciaires, et [le] rôle respectif qu'elles ont chacune à assurer en principe »[1557]. L'importance de cette distinction s'explique dans la mesure où le contentieux relatif aux activités de police administrative relève du juge administratif tandis que celui de la police judiciaire est de la compétence du juge judiciaire[1558]. En outre, les activités relevant de la police judiciaire s'effectuent sous le contrôle d'un magistrat[1559] car elles ont une vocation répressive et peuvent conduire à une plus grande restriction des libertés, à l'image des prises de vue de l'intérieur d'un domicile[1560]. À l'inverse, les activités relevant de la police administrative reposent sur un objectif de prévention des infractions susceptibles de conduire à un trouble de l'ordre public[1561]. Les deux types de police sont

---

1555 Loi des 16 et 24 août 1790 sur l'organisation judiciaire, art. 13 [en ligne] : « Les fonctions judiciaires sont distinctes et demeureront toujours séparées des fonctions administratives. Les juges ne pourront, à peine de forfaiture, troubler, de quelque manière que ce soit, les opérations des corps administratifs, ni citer devant eux les administrateurs pour raison de leurs fonctions » ; Décret du 2 septembre 1795 (16 fructidor an III) qui défend aux tribunaux de connaître des actes d'administration, et annule toutes procédures et jugements intervenus à cet égard [en ligne] : « Défenses itératives sont faites aux tribunaux de connaître des actes d'administration, de quelque espèce qu'ils soient, aux peines de droit ».

1556 C. const., Décision n° 86-224 DC, 23 janvier 1987, *Loi transférant à la juridiction judiciaire le contentieux des décisions du Conseil de la concurrence*, Rec. p. 8, spéc. cons. 15 et 16 [en ligne].

1557 PETIT (J.) et FRIER (P-L.), *Droit administratif*, Paris, LGDJ, 2022, 812 p., p. 342. Voir aussi : BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 703 : « Historiquement, la distinction est née de la nécessité de déterminer *ex post* l'ordre de juridiction compétent pour juger de la réparation des dommages issus d'une opération de police ».

1558 GAUDEMET (Y.), *Droit administratif*, *op. cit.*, p. 388. Voir également : DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, Paris, Dalloz, 14ème édition, 2021, 690 p., p. 365 : « le juge administratif est compétent pour annuler une décision de police administrative, et pour en réparer les conséquences ; le juge judiciaire peut seul procéder à l'indemnisation des victimes d'opérations de police judiciaire ».

1559 PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 343.

1560 Voir à titre d'exemple l'arrêt du juge judiciaire concernant des opérations de captation d'images par drones aériens au dessus d'une propriété privée à des fins de lutte contre le trafic de stupéfiants (C. cass., ch. crim., 15 novembre 2022, n° 22-80.097, *op. cit.*).

1561 Voir notamment : CE, 10ème et 9ème Sect., 9 novembre 2015, n° 376107, *Alliance générale contre le racisme et le respect de l'identité française et chrétienne*, §6 [en ligne] : « il appartient à l'autorité investie du pouvoir de police administrative de prendre les mesures nécessaires, adaptées et proportionnées pour prévenir la commission des infractions pénales susceptibles de constituer un trouble à l'ordre public sans porter d'atteinte excessive à l'exercice par les citoyens de leurs libertés fondamentales ».

ainsi complémentaires par le lien entretenu entre « la commission d'une infraction et l'existence d'un trouble à l'ordre public »[1562].

571. Les critères permettant de distinguer les deux formes de police ont été précisés par le juge administratif dans l'arrêt *Baud* du 11 mai 1951 précisant que « toute opération de recherche des infractions et de poursuite de leurs auteurs est une opération de police judiciaire »[1563]. Dans sa décision du 7 juin 1951[1564], le Tribunal des conflits a également participé à éclaircir cette distinction en énonçant que les opérations qui n'entrent pas dans le cadre de la répression d'une infraction déterminée mais exécutent une mission de contrôle et de surveillance relèvent de la police administrative. Toutefois, l'application des principes de distinction n'est pas toujours aisée étant donné que des infractions peuvent être commises lors d'une opération de police administrative[1565] et que dans certaines opérations les deux finalités semblent être mêlées[1566].

572. Ainsi, la distinction entre les deux formes de police se révèle parfois complexe à établir à deux égards. D'une part, une personne représentante des forces de l'ordre peut exercer ses missions autant en tant qu'autorité de police administrative qu'en tant qu'autorité de police judiciaire[1567]. Marc-Antoine Granger rappelait aussi que « si une même mesure de police ne peut être simultanément acte de police judiciaire et acte de police administrative, la mutabilité des opérations de police est en revanche possible »[1568]. D'autre part, la personne agissant en tant qu'autorité de police administrative a le devoir de mettre fin aux troubles à l'ordre public dont elle est témoin[1569]. Afin de déterminer la qualification à donner à l'opération et éviter un contentieux entre le juge

---

[1562] DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 364.

[1563] CE, sect., 11 mai 1951, n° 2542, *Baud*, Rec. p. 265.

[1564] TC, 7 juin 1951, Décision n° 1.316, *Dame Noualek*, Rec. p. 636

[1565] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 343 : « toute action de répression peut aussi prévenir un trouble et inversement ». Voir à titre d'exemple : TC, 5 décembre 1977, Décision n° 02060, *Demoiselle Motsch*, Rec. p. 671 [en ligne] ; TC, 12 juin 1978, *Société « Le profil »*, Rec. p. 648 [en ligne] ; TC, 15 janvier 1968, Décision n° 01909, *Consorts Tayeb*, Rec. p. 791 [en ligne].

[1566] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 344 ; DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 364 : « une même opération peut revêtir successivement les caractères d'opération de police administrative, puis judiciaire ».

[1567] GAUDEMET (Y.), *Droit administratif*, *op. cit.*, p. 389 : « les deux pouvoirs peuvent être confiés à un même titulaire et c'est souvent le cas : le maire est à la fois sous la surveillance du procureur de la République, officier de police judiciaire, et autorité de police administrative de et dans la commune ».

[1568] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 65.

[1569] DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 364.

judiciaire et le juge administratif, les juges se fondent sur « l'objectif principal », en d'autres termes sur l'objectif essentiel de l'action[1570].

573. Toutefois, le constat a maintes fois été observé d'une atténuation progressive de la distinction entre les missions relevant de la police administrative et celles attribuées à la police judiciaire[1571]. En ce sens, Marc-Antoine Granger soulignait que « toute la police administrative n'est pas préventive et elle n'est pas la seule à pouvoir l'être »[1572]. De manière similaire, la professeure Raphaële Parisot affirmait que « si le code de la sécurité intérieure renvoie bien, en principe, pour les missions de police judiciaire assurées par la police et la gendarmerie nationale au Code de procédure pénale[1573] […], il prévoit aussi que des actes puissent relever de la police administrative comme de la police judiciaire : tel est le cas de l'utilisation de caméras mobiles par les agents de la police nationale et les militaires de la gendarmerie nationale[1574] »[1575].

574. Les mesures de prévention des actes de terrorisme tendent à accentuer le phénomène d'effacement des frontières traditionnellement admises entre la police administrative et la police judiciaire[1576] notamment par l'intermédiaire des systèmes de vidéoprotection[1577]. En ce sens,

---

[1570] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 344 ; DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 364.

[1571] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, spéc. pp. 191-222.

[1572] *Idem*, p. 209.

[1573] CSI, art. L. 411-1 : « La police nationale relève de l'autorité du ministre de l'intérieur, sous réserve des dispositions du code de procédure pénale relatives à l'exercice de la police judiciaire » ; CSI art. L. 421-1 et L. 421-2 : « La police judiciaire constitue l'une [des] missions essentielles » de la gendarmerie nationale qui « est placée sous l'autorité du ministre de l'Intérieur, responsable de son organisation, de sa gestion, de sa mise en condition d'emploi et de l'infrastructure militaire qui lui est nécessaire ».

[1574] CSI, art. L. 241-1, al. 1er : « Dans l'exercice de leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens ainsi que de leurs missions de police judiciaire, les agents de la police nationale et les militaires de la gendarmerie nationale peuvent procéder en tous lieux, au moyen de caméras individuelles, à un enregistrement audiovisuel de leurs interventions lorsque se produit ou est susceptible de se produire un incident, eu égard aux circonstances de l'intervention ou au comportement des personnes concernées ».

[1575] PARIZOT (R.), « La distinction entre police administrative et police judiciaire est-elle dépassée ? », pp. 133-145, spéc. pp. 137-138 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*

[1576] Voir notamment : ALIX (J.), « La lutte contre le terrorisme entre prévention pénale et prévention administrative », *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, op. cit., pp. 147-158, spéc. p. 147 : « La prévention du terrorisme, qui repose sur une répartition très incertaine entre les aspects pénaux et les aspects administratifs de la question, illustre parfaitement la confusion entre finalité répressive et finalité préventive, mais aussi entre outils de prévention et outils de répression, de sorte que les codes pénaux sont bien trop souvent préventif, et le Code de la sécurité intérieure se fait progressivement instrument répressif ».

[1577] La LOPS du 25 janvier 1995 a introduit la prévention de la lutte contre le terrorisme au sein de la liste des motifs permettant l'utilisation de systèmes de vidéoprotection sur la voie publique (CSI, art. L. 251-2 6° [caméras fixes de vidéoprotection] et art. L. 242-5 3°) [caméras aéroportées]).

Pauline Gervier soulignait que l'entremêlement entre les finalités préventives et répressives était d'autant plus marqué s'agissant des mesures en matière de lutte contre le terrorisme[1578]. De fait, la lutte contre le terrorisme ne pouvant être appréhendée efficacement que de manière globale a favorisé ce phénomène visant à étendre le champ d'action des différents acteurs de la force publique allant jusqu'à « brouiller » les frontières entre l'exercice des missions de sécurité sur le territoire national (sécurité intérieure) et les missions relevant du cadre de la sécurité extérieure[1579]. Les technologies de surveillance de sécurité publique, notamment les systèmes de vidéoprotection, n'ont fait qu'amplifier cet effet d'effacement des frontières entre actions préventives et répressives[1580]. Dans sa thèse, Marc-Antoine Granger affirmait ainsi que « la prévention des infractions implique nécessairement la recherche de comportements qui laissent présager la commission de ces infractions »[1581]. Les systèmes de vidéoprotection reposent sur des finalités de nature hybride[1582]. En outre, leur association à des algorithmes d'analyse d'évènements à des fins de détection de comportements anormaux (de personnes potentiellement dangereuses) ou de missions générales de préservation de l'ordre public (police administrative) ou encore de missions de recherche des auteurs d'infractions (police judiciaire) pourrait brouiller davantage la frontière originairement établie entre les finalités préventives et répressives.

575. Cette distinction entre police judiciaire et police administrative, qui se justifiait autrefois, ne semble dès lors plus être aussi pertinente et adaptée aujourd'hui compte tenu notamment de l'amplification des usages technologiques par les forces de l'ordre qui entremêlent prévention et constatation des infractions[1583]. Il en va encore plus ainsi s'agissant des drones aériens de sécurité publique qui introduisent une recherche coercitive d'infractions y compris dans un cadre de police

---

[1578] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, spéc. pp. 132-133.

[1579] En ce sens, le Livre blanc de 2008 sur la défense et la sécurité nationale énonçait que « la distinction entre sécurité intérieure et sécurité extérieure n'[était] plus pertinente » (Ministère de la Défense, Rapport « Livre blanc sur la défense et la sécurité nationale 2008 » remis par MALLET (J-C.), 17 juin 2008, 402 p., p. 57 [en ligne]).

[1580] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 210 : Quant aux dispositifs de vidéoprotection, leur vertu préventive est limitée en ce qu'elle se borne à dissuader les auteurs d'infractions par le risque d'être vus et identifiés. Le reste du temps […] l'intention des agents qui surveillent les images des moniteurs est de prendre sur le fait les auteurs d'infractions ».

[1581] *Idem*, pp. 209-210.

[1582] CSI, art. L. 251-2 6° (caméras fixes) et art. L. 242-5 3°) (caméras aéroportées).

[1583] PARIZOT (R.), « La distinction entre police administrative et police judiciaire est-elle dépassée ? », pp. 133-145, spéc. p. 140 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.* : « Le droit pénal intervient de manière toujours plus précoce, et une personne évaluée comme représentant une menace peut être considérée, dans bien des hypothèses, comme un simple sujet à risque (relevant donc de la police administrative) ou bien comme un véritable délinquant (relevant alors du droit pénal) ».

administrative[1584]. L'atténuation de cette distinction pourrait même affaiblir les garanties des droits et libertés « dans la mesure où elle permet, fort commodément, de se détacher des règles protectrices de procédure pénale »[1585]. De surcroît, l'association d'algorithmes d'aide à la prise de décision aux technologies de surveillance de sécurité publique questionne davantage la légitimité des forces de l'ordre à faire usage de ces outils toujours plus intrusifs au motif de vouloir renforcer la sécurité des personnes et des biens.

B. La légitimité relative du recours aux technologies de surveillance « augmentées » de sécurité publique

576. Le recours à des technologies « augmentées » par les forces de l'ordre et les services de secours entend répondre à différentes finalités légitimes de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, d'une part, et de secours aux personnes, d'autre part. Néanmoins, leur utilisation à des fins préventives soulève encore de nombreux enjeux, notamment quant aux risques d'erreurs de l'algorithme dans l'interprétation des évènements filmés par une caméra de vidéoprotection ou encore dans l'identification de la personne filmée[1586] (v. **n° 377 et suiv.**). Dès lors, les algorithmes d'aide à la prise de décision, dont seront équipés les drones aériens de sécurité publique, pourraient avoir des effets particulièrement néfastes dans certains choix de présentation des résultats[1587].

577. En outre, le fait que les décisions prises par les forces de l'ordre reposent, même seulement partiellement, sur les résultats produits par un algorithme soulève des enjeux quant au maintien du caractère régalien des activités de sécurité publique. De fait, le recours à des outils d'aide à la prise de décision conçus par des entreprises privées questionne la légitimité de leur utilisation par les forces de l'ordre, seules détentrices des pouvoirs de police inhérents à la puissance régalienne (v. **n° 442 et suiv.**). En ce sens, le Conseil d'État avait souligné, dans son

---

[1584] BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, pp. 11-15, spéc. p. 13.

[1585] PARIZOT (R.), « La distinction entre police administrative et police judiciaire est-elle dépassée ? », pp. 133-145, spéc. p. 144 *in* TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, *op. cit.*

[1586] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 56 : « La question de la légitimité se pose […] quand l'usage d'un SAAD peut avoir des effets indirects, ou secondaires, sur la vie en société ».

[1587] *Idem*, p. 70.

rapport annuel de 2017, le fait que « les administrations ne sont pas non plus à l'abri de la concurrence des plateformes numériques dans l'exercice des fonctions de sécurité et de justice »[1588].

578. Aussi, le fondement des modèles algorithmiques, élaboré par des entités privées, pourrait remettre en cause la légitimité du recours à cette technologie notamment lorsque celui-ci ne repose sur aucune base scientifique établie[1589]. En outre, la question de la légitimité de l'emploi d'algorithmes « augmentés » se pose plus particulièrement s'agissant des critères sur lesquels reposent leurs résultats[1590]. La détection automatique de comportements anormaux prêterait ainsi à controverse compte tenu des difficultés à établir ce qu'est un comportement anormal[1591]. Le fait d'adopter une perception particulière pourrait avoir pour effet d'uniformiser les comportements des personnes qui chercheraient à rester anonymes aux « yeux » des caméras ou du moins de ne pas « attirer leur attention ». Ce constat avait notamment été souligné par la CNIL qui souhaitait que soit tenu un débat démocratique sur les nouveaux usages des caméras vidéo[1592]. Le recours à ce type d'algorithmes ouvre ainsi le débat concernant la responsabilité (en cas d'erreur dans la prise de décision) des différents acteurs impliqués durant la « vie de l'algorithme » dont une part pourrait dépendre de son processus de programmation (v. **n° 692 et suiv.**).

579. Enfin, la transparence[1593] de leur usage constitue un des enjeux majeurs des algorithmes d'aide à la prise de décision, particulièrement s'agissant des autorités publiques. La légitimité quant à l'utilisation des algorithmes par les forces de l'ordre réside dans la connaissance de leur usage par les personnes concernées, qui est étroitement liée au droit à l'information des personnes dans le

---

1588 CE, Étude annuelle 2017 sur « Puissance publique et plateforme numériques : accompagner l'ubérisation », 13 juillet 2017 [en ligne].

1589 FELDMAN BARRETT (L.), *How Emotions Are Made: the Secret Life of the Brain*, New York, Houghton Mifflin Harcourt. [2017] ; LERNER (J.S.), LI (Y.), VALDESOLO (P.) and KASSAM (K.S.), "Emotion and decision-making", *Annual Review of Psychology*, 66, 2015, pp. 799-823 [en ligne] ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 71 ; STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *op. cit.*, pp. 38-39.

1590 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 56.

1591 LAVENUE (J-J.), « Anormalité, surveillance et fichiers de police » *in* LAVENUE (J-J.) et VILLABA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, *op. cit.*, pp. 235-260, spéc. pp. 245-246.

1592 CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018 [en ligne] ; CNIL, « Reconnaissance faciale - Pour un débat à la hauteur des enjeux », 15 novembre 2019, 11 p. [en ligne].

1593 COURTOIS (G.) et GOSSE (N.), « Enjeux juridiques et éthiques des algorithmes », *Revue de la gendarmerie national « Algorithmes et espace normatif »*, 2nd Trimestre 2018, p. 86 [en ligne].

cadre du traitement de leur DACP. Néanmoins, ce principe de transparence du recours à des algorithmes se confronte à des exceptions dans le cadre des procédures pénales dérogatoires relatives à la lutte contre la criminalité organisée et le terrorisme.

CHAPITRE 2 LA REDÉFINITION DES GARANTIES DU RAPPORT SÛRETÉ-SÉCURITÉ À L'ÈRE DES DRONES AÉRIENS « AUGMENTÉS » DE SÉCURITÉ PUBLIQUE

580. Au sein d'un État de droit, le juge joue un rôle essentiel garantissant l'exercice des droits et libertés tant contre la puissance publique que contre leur violation par des tiers[1594]. En France, plusieurs juridictions nationales sont compétentes pour tenter de maintenir une protection effective des droits et libertés impliqués dans le rapport sûreté-sécurité. En premier lieu, le juge judiciaire et le juge administratif se répartissent le contentieux. En deuxième lieu, le Conseil constitutionnel intronisé avec la Constitution de 1958, opère le contrôle de la constitutionnalité des textes législatifs. Les technologies occupent une large place au sein de la jurisprudence des trois juridictions. La législation autant que les mesures de police portant sur les technologies de surveillance de sécurité publique ont ainsi contribué au développement d'une jurisprudence dont les solutions laissent apparaître un certain affaiblissement des garanties des droits et libertés (**Section 1**).

581. Outre les juridictions nationales, la protection des droits et libertés fait également l'objet d'une jurisprudence croissante des juridictions européennes composées de la CEDH, d'une part, et de la CJUE, d'autre part. L'emprise grandissante des nouvelles technologies sur la société a déjà conduit les deux juridictions à rendre des décisions concernant leur emploi. Elles se sont notamment illustrées concernant des affaires portant sur le recours à des technologies par les forces de l'ordre à des fins de surveillance. Enfin, dans le cadre des efforts menés par l'État pour encadrer les dispositions législatives et les mesures prises par les autorités en matière de sécurité publique, plusieurs institutions non-juridictionnelles ont progressivement vu le jour aux fins de participer à la garantie des droits et libertés. Les AAI endossent ainsi des compétences spécifiques à certains domaines leur permettant d'avoir une meilleure appréhension des sujets à traiter. En matière de technologies de surveillance de sécurité publique, la CNIL exerce un rôle de premier plan. Dans cette tâche le Défenseur des droits est lui aussi acteur prépondérant (**Section 2**).

[1594] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 261.

Section 1 L'affaiblissement des garanties des droits et libertés à l'ère des technologies de surveillance de sécurité publique

582. En France, les acteurs juridictionnels ont un rôle essentiel pour assurer la protection des droits et libertés dans le cadre de l'utilisation de technologies de surveillance de sécurité publique. Depuis la loi des 16 et 24 août 1790 et le décret du 2 septembre 1795[1595], l'organisation juridictionnelle française est scindée entre le juge judiciaire et le juge administratif qui garantissent l'un comme l'autre le respect des droits et libertés[1596]. Ces deux juridictions assurent respectivement le contrôle des mesures de police judiciaire et de police administrative. Dans la course à l'emploi des technologies de surveillance par les forces de l'ordre, les deux juridictions ont eu l'occasion de rendre des décisions assurant de manière plus ou moins convaincante une garantie effective des droits et libertés impliqués (§2). Le Conseil constitutionnel constitue la troisième force juridictionnelle de protection des droits et libertés en France. Face à l'engouement des politiques sécuritaires pour les technologies de surveillance de sécurité publique, il joue, lui aussi, un rôle primordial dans leur processus d'encadrement (§1).

§1. La protection déclinante du juge constitutionnel confronté aux technologies de surveillance de sécurité publique

583. Depuis sa création en 1958, le Conseil constitutionnel est reconnu comme le protecteur des droits et libertés[1597] dans la mesure où il assure un contrôle de conformité de la législation au bloc de constitutionnalité[1598]. Le juge constitutionnel a su s'imposer comme un des acteurs essentiels du rapport sûreté-sécurité, notamment par ses décisions portant sur son contrôle de constitutionnalité des lois relatives à l'emploi de technologies de sécurité publique. Cependant, ses décisions en la matière font souvent l'objet de critiques évoquant la marge de manœuvre trop importante laissée aux autorités publiques sous le prétexte de vouloir répondre aux enjeux sociétaux

---

[1595] Loi des 16 et 24 août 1790 sur l'organisation judiciaire, *op. cit.*, art. 13 ; Décret du 2 septembre 1795 (16 fructidor an III) qui défend aux tribunaux de connaître des actes d'administration, et annule toutes procédures et jugements intervenus à cet égard, *op. cit.*, article unique.

[1596] C. const., Décision n° 89-261 DC, 28 juillet 1989, *Loi relative aux conditions de séjour et d'entrée des étrangers en France*, Rec. p. 81, cons. 29 [en ligne] : « la garantie effective des droits des intéressés […] peut être satisfaite aussi bien par la juridiction judiciaire que par la juridiction administrative ».

[1597] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 97 ; LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, op. cit., p. 109.

[1598] Constitution de 1958, art. 61.

d'« insécurité » (A). Lors de l'adoption du texte de la loi JOP2024, le juge constitutionnel a une nouvelle fois été saisi afin d'effectuer un contrôle *a priori* de l'adéquation de ces dispositions au bloc de constitutionnalité. Toutefois, sa décision peine à convaincre et à offrir une garantie effective des droits et libertés quant au recours à des technologies « augmentées » par les forces de l'ordre (B).

A. Les pouvoirs limités du juge constitutionnel pour garantir les droits et libertés face aux restrictions posées par les caméras de surveillance de sécurité publique

584. À l'origine, le Conseil constitutionnel avait pour seule compétence d'assurer le contrôle « de l'activité des pouvoirs publics »[1599]. Il s'érigera progressivement en gardien des droits et libertés suite à plusieurs évènements ayant marqué le droit constitutionnel[1600]. En premier lieu, lors de la décision *Liberté d'association* du 16 juillet 1971, le juge constitutionnel a interprété, pour la première fois, de manière extensive les dispositions de la Constitution relative à l'édification des lois et pris la décision de contrôler la loi au regard du respect des droits et libertés consacrés par les textes constitutionnels *lato sensu*[1601]. Cette décision démontre l'indépendance du Conseil constitutionnel qui initia la référence au bloc de constitutionnalité. En deuxième lieu, la révision constitutionnelle du 29 octobre 1974 a permis d'étendre le droit de saisine du Conseil constitutionnel (initialement réservé au président de la République, au Premier ministre, au président du Sénat et au président de l'Assemblée nationale) à la minorité parlementaire composée de soixante députés ou de soixante sénateurs[1602]. Le Conseil constitutionnel n'étant pas en mesure de s'auto-saisir, la révision de ce droit confère un pouvoir à l'opposition et a conduit à une extension du contentieux constitutionnel. En dernier lieu, le dispositif de contrôle du juge

---

[1599] C. const., Décision n° 62-20 DC, 6 novembre 1962, *Loi relative à l'élection du Président de la République au suffrage universel direct, adoptée par le référendum du 28 octobre 1962*, Rec. p. 27, cons. 1-5 [en ligne].

[1600] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 302 : « l'établissement du "bloc de constitutionnalité", la mise en place de méthodes de jugement et d'une jurisprudence, d'une déontologie de l'institution, tout concours à en faire un des principaux rouages de l'État de droit ». Voir aussi : Conseil constitutionnel, « Les droits et libertés » [en ligne].

[1601] C. const., Décision n° 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association*, *op. cit.*, cons. 2.

[1602] Loi constitutionnelle n° 74-904 du 29 octobre 1974 portant révision de l'article 61 de la Constitution, *JORF* du 30 octobre 1974, article unique [en ligne].

constitutionnel a été complété par la révision constitutionnelle du 23 juillet 2008[1603] et la loi organique du 10 décembre 2009[1604] introduisant une nouvelle forme d'exception d'inconstitutionnalité en vue de renforcer les garanties des droits et libertés : la question prioritaire de constitutionnalité (QPC). Elle permet à tout justiciable de contester une disposition législative, qui lui serait applicable devant les juridictions nationales, dès lors qu'il considère qu'elle porte atteinte aux droits et libertés garantis par le bloc de constitutionnalité par renvoi de la Cour de cassation ou du Conseil d'État et que la question n'a pas été préalablement traitée par le Conseil constitutionnel[1605]. Dès lors, l'introduction de ce pouvoir du juge constitutionnel ouvre la possibilité de contester la constitutionnalité de textes n'ayant pas fait l'objet de son contrôle *a priori* notamment en matière de sécurité publique (ex. garde à vue), tels que ceux adoptés avant 2008.

585. Les pouvoirs du Conseil constitutionnel lui permettent ainsi d'exercer un contrôle *a priori* et *a posteriori* des dispositions législatives qui sont soumises à son examen en vue de renforcer concrètement la protection des droits et libertés. En d'autres termes, le juge constitutionnel est compétent pour contrôler les lois avant leur promulgation mais aussi après leur adoption, sous réserve qu'elles n'aient pas déjà fait l'objet d'un contrôle *a priori*[1606]. Toutefois, ses pouvoirs sont limités dans la mesure où son contrôle *a priori* des dispositions législatives est essentiellement facultatif[1607] à l'exception des lois organiques[1608]. C'est ainsi qu'en matière de lois « sécuritaires », le juge constitutionnel a été saisi de manière presque systématique afin d'effectuer un contrôle de constitutionnalité préalablement à leur promulgation à l'exception de la loi sur la sécurité quotidienne[1609], dont plusieurs dispositions auraient pourtant pu être déclarées comme étant

---

[1603] Loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la Ve République, *JORF* n°0171 du 24 juillet 2008, art. 29 [en ligne] : Elle a introduit l'article 61-1 dans la Constitution qui dispose que « lorsque, à l'occasion d'une instance en cours devant une juridiction, il est soutenu qu'une disposition législative porte atteinte aux droits et libertés que la Constitution garantit, le Conseil constitutionnel peut être saisi de cette question sur renvoi du Conseil d'État ou de la Cour de cassation qui se prononce dans un délai déterminé ».

[1604] Loi organique n° 2009-1523 du 10 décembre 2009 relative à l'application de l'article 61-1 de la Constitution, *JORF* n°0287 du 11 décembre 2009 [en ligne].

[1605] Constitution de 1958, art. 61-1.

[1606] Ordonnance n° 58-1067 du 7 novembre 1958 portant loi organique sur le Conseil constitutionnel, *JORF* du 9 novembre 1958 (révisée par la loi organique n° 2009-1523 du 10 décembre 2009), art. 23-2 2° [en ligne].

[1607] Constitution de 1958, art. 61 §2.

[1608] *Idem*, art. 61 §1.

[1609] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *op. cit.*

contraires à la Constitution[1610].

586. Le contentieux constitutionnel comprend de nombreuses décisions portant sur les dispositions législatives relatives aux caméras de surveillance de sécurité publique suite aux saisines systématiques des parlementaires[1611]. Ces décisions ont souvent fait l'objet de critiques (v. **Partie 1**). De fait, les lois en matière de sécurité font l'objet d'une jurisprudence importante du Conseil constitutionnel qui consiste le plus souvent à s'assurer que l'atteinte portée aux droits et libertés au nom de la sauvegarde de l'ordre public n'est pas « manifestement déséquilibrée »[1612]. En règle générale, lorsqu'il contrôle un texte de loi dans ce domaine, il se contente d'opérer « la balance entre d'une part la nécessité de garantir [le] droit fondamental [avancé] et d'autre part celle de préserver l'exigence de sauvegarde de l'ordre public »[1613]. En d'autres termes, il s'assure uniquement que le législateur a opéré une conciliation entre le droit ou la liberté en cause et les contraintes imposées par l'ordre public[1614]. Ce contrôle opérant une simple détermination de conciliation est récurrent dans la jurisprudence constitutionnelle notamment s'agissant des dispositions relatives aux dispositifs de traitement de DACP par les forces de l'ordre[1615]. Dès lors, le Conseil constitutionnel se montre globalement malléable à l'égard des lois en matière de sécurité[1616].

587. La jurisprudence du Conseil constitutionnel fait néanmoins apparaître une constance dans sa volonté d'interdire toute forme de délégation de pouvoirs de police à des personnes privées, notamment en matière de vidéoprotection. En ce sens, dans sa décision du 10 mars 2011, il s'est

---

[1610] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 126.

[1611] C. const., Décision n° 94-352 DC, 18 janvier 1995 (LOPS), *op. cit.* ; C. const., Décision n° 2011-625 DC, 10 mars 2011 (LOPPSI), *op. cit.* ; C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.* ; C. const., Décision n° 2021-834 DC, 20 janvier 2022 (RPSI), *op. cit.*

[1612] VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 95.

[1613] FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, *op. cit.*, p. 579.

[1614] De manière non-exhaustive : *Ibid* ; DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, *op. cit.*, spéc. p. 101 ; GOHIN (O.), « La sécurité dans la Constitution de 1958 », *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, *op. cit.*, pp. 19-29, spéc. p. 28.

[1615] Voir par exemple : C. const., Décision n° 94-352 DC, 18 janvier 1995 (LOPS), *op. cit.*, cons. 16 (vidéosurveillance) ; C. const., Décision n° 2011-625 DC, 10 mars 2011 (LOPPSI), *op. cit.*, cons. 70-72 (fichiers de police) ;

[1616] PERERA (S.), *Le principe de liberté en droit public français*, *op. cit.*, p. 222 ; VIDAL-NAQUET (A.), « La sécurité en droit constitutionnel : non-dit ou non-être ? », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 79-102, spéc. p. 96.

référé à l'article 12 de la DDHC afin d'affirmer l'interdiction de déléguer à des personnes privées « des compétences de police administrative générale inhérentes à l'exercice de la "force publique" nécessaire à la garantie des droits »[1617]. En d'autres termes, les Sages ont estimé que le contrat social unissant l'État à ses citoyens exige que la puissance publique assure ses responsabilités[1618] (v. **n° 419 et suiv.**).

588. Aussi, le Conseil constitutionnel a su se montrer vigilant, dans un premier temps, à l'égard de l'emploi de drones aériens par les forces de l'ordre lorsqu'il a déclaré les dispositions y afférents, issues de la loi pour une sécurité globale préservant les libertés, contraires à la Constitution au motif qu'elles portaient une atteinte disproportionnée au droit à la vie privée[1619]. Pourtant, il a fini par céder à la demande du législateur lorsque les dispositions, révisées par la loi RPSI, ont été de nouveau soumises à son contrôle de constitutionnalité[1620]. Afin de garantir au mieux le droit à la vie privée (seul droit mis en cause), il a formulé plusieurs réserves d'interprétation concernant le renouvellement de l'autorisation de recours à des drones aériens[1621] telle que l'exclusion formelle de tout « rapprochement, interconnexion ou mise en relation automatisée » des données collectées par les drones aériens de sécurité publique « avec d'autres données à caractère personnel »[1622]. En outre, il a rejeté la disposition autorisant le recours à ces dispositifs en cas d'urgence pour une durée pouvant atteindre quatre heures et à la seule condition d'en avoir préalablement informé le préfet[1623].

589. Dernièrement, c'est à l'occasion du vote de la loi JOP2024, adoptant des dispositions en matière d'utilisation expérimentale de caméras « augmentées » de sécurité publique, que le Conseil constitutionnel a une nouvelle fois eu l'occasion de rendre une décision concernant le recours à des

---

[1617] C. const., Décision n° 2011-625 DC, 10 mars 2011, *op. cit.*, cons. 18 et 19 : « en confiant à des opérateurs privés le soin d'exploiter des systèmes de vidéoprotection sur la voie publique et de visionner les images pour le compte de personnes publiques, les dispositions contestées permettent d'investir des personnes privées de missions de surveillance générale de la voie publique ».

[1618] WACHSMANN (P.), *Libertés publiques*, *op. cit.*, p. 10.

[1619] C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.*, cons. 148.

[1620] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 46.

[1621] *Idem*, cons. 28.

[1622] *Idem*, cons. 30.

[1623] *Idem*, cons. 31 : « ces dispositions permettent le déploiement de caméras aéroportées, pendant une telle durée, sans autorisation du préfet, sans le réserver à des cas précis et d'une particulière gravité, et sans définir les informations qui doivent être portées à la connaissance de ce dernier. Dès lors, elles n'assurent pas une conciliation équilibrée entre les exigences constitutionnelles précitées ».

dispositifs de vidéoprotection.

B. Les caméras « augmentées » de sécurité publique devant le juge constitutionnel : une protection perfectible des droits et libertés

590. La décision du Conseil constitutionnel du 17 mai 2023 portant sur le contrôle de la loi JOP2024[1624] était très attendue compte tenu de la sensibilité que présente le recours à des algorithmes d'analyse d'images de caméras de surveillance par les forces de l'ordre[1625]. À cette occasion, le juge constitutionnel a validé les dispositions portant sur le recours, à titre expérimental, au traitement algorithmique d'images de caméras fixes et de drones aériens de vidéoprotection à des fins de détection et de signalement d'évènements[1626]. Il a assorti sa décision de conformité à la Constitution de deux réserves d'interprétation. La première ne constitue qu'une formulation classique de sa procédure de contrôle rappelant au législateur son obligation d'assortir de garanties des droits et libertés l'emploi de cette technologie ainsi que d'assurer la conciliation entre l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public et le droit à la vie privée[1627]. Néanmoins, il a précisé que le caractère particulièrement intrusif du recours à cette technologie dépassant celle de la simple collecte d'images nécessite de la part du législateur l'adoption de garanties spécifiques assurant la sauvegarde du droit à la vie privée[1628].

591. Dans sa décision, le Conseil constitutionnel a rejeté le motif selon lequel « la détection de certains événements conduirait nécessairement au traitement de données biométriques alors même que la loi l'interdit »[1629]. Il a justifié sa position en rappelant qu'effectivement « les

---

[1624] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.*

[1625] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.* ; COURRÈGES (A.), « Le Conseil constitutionnel apporte des précisions inédites à l'occasion de l'examen de la loi relative aux jeux Olympiques et Paralympiques de 2024 », *DA* n° 7, 1er juillet 2023, 80.

[1626] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.*, cons. 46 et 49.

[1627] *Idem*, cons. 32.

[1628] *Idem*, cons. 33 : « Pour répondre à l'objectif de valeur constitutionnelle de prévention des atteintes à l'ordre public, le législateur peut autoriser le traitement algorithmique des images collectées au moyen d'un système de vidéoprotection ou de caméras installées sur des aéronefs. Si un tel traitement n'a ni pour objet ni pour effet de modifier les conditions dans lesquelles ces images sont collectées, il procède toutefois à une analyse systématique et automatisée de ces images de nature à augmenter considérablement le nombre et la précision des informations qui peuvent en être extraites. Dès lors, la mise en œuvre de tels systèmes de surveillance doit être assortie de garanties particulières de nature à sauvegarder le droit au respect de la vie privée ».

[1629] *Idem*, cons. 29.

dispositions contestées prévoient que les traitements algorithmiques […] n'utilisent aucun système d'identification biométrique et ne recourent pas à des données biométriques »[1630]. Les inquiétudes formulées[1631] quant à la possibilité que les caméras « augmentées » prévues par la loi JOP2024 puissent recourir à des algorithmiques d'analyse de DACP biométriques semblent être ici écartées. Aussi, le Conseil constitutionnel a considéré que les dispositions relatives à l'information du public concernant l'usage de traitements algorithmiques des images de vidéoprotection[1632] respectaient le devoir d'information des personnes concernées[1633]. Pourtant, le caractère imprécis des modalités concrètes d'information du public s'agissant du recours à des drones aériens « augmentés » laisse craindre une absence de garantie effective du droit à l'information des personnes concernées par les traitements de DACP, à l'instar des dispositions de la loi RPSI et de son décret d'application (v. **n° 230-231**). En ce sens, le décret publié le 28 août 2023 portant sur l'article 10 de la loi JOP2024 n'offre pas davantage de précisions concernant les mesures « pratiques » permettant la mise en œuvre de cette information[1634].

592. Il convient de noter que le juge constitutionnel a donné son aval à l'usage de technologies intrusives dès la première soumission du législateur sans même avoir demandé de précisions quant aux évènements susceptibles de faire l'objet de cette expérimentation[1635]. Pourtant, le titre du texte s'avère trompeur en induisant que ses dispositions ne porteraient que sur la période des JOP 2024. Or, le texte se prolonge bien au-delà des JOP 2024 tant en termes de durée des dispositions à caractère expérimental (limitées dans le temps)[1636] que des autres dispositions,

---

[1630] *Idem*, cons. 42.

[1631] Voir notamment : BERTRAND (B.), « Encadrement des technologies de surveillance : les enseignements de l'expérimentation des JO 2024 », *op. cit.*

[1632] Loi JOP2024, art. 10 III.

[1633] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit*., cons. 40.

[1634] Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *JORF* n°0200 du 30 août 2023, art. 17, II [en ligne].

[1635] Il rejette la requête selon laquelle « ces dispositions seraient entachées d'incompétence négative faute de définir les événements que les traitements algorithmiques ont pour objet de détecter, les situations dans lesquelles ils peuvent être utilisés et les conditions d'habilitation et de formation des agents en faisant usage » (*Idem*, cons. 28)

[1636] La durée des dispositions expérimentales portant sur le recours à des caméras « augmentées » courant de la date d'exécution du texte de loi (le 20 mai 2023) au 31 mars 2025 (Loi JOP 2024, art. 10, I).

certaines d'entre elles entrant directement dans le droit commun ainsi que l'avait souligné le Conseil d'État dans son avis rendu en décembre 2022[1637].

593. D'une manière générale, la décision du Conseil constitutionnel ne surprend pas. Toutefois, il est regrettable que le Conseil n'ait pas relevé le caractère disproportionné[1638] de la durée de l'expérimentation, dont la fin a été fixée en dernier lieu au 31 mars 2025[1639], se satisfaisant de la simple inscription de la durée maximale de l'expérimentation au sein des dispositions de l'article 10 de la loi JOP2024 par le législateur[1640]. Aussi, il peut être reproché aux Sages de ne pas avoir souligné le caractère pour le moins imprécis des évènements susceptibles de faire l'objet d'un traitement algorithmique d'analyse d'images de vidéoprotection[1641] notamment au regard de l'étendue de la durée d'application de ces dispositions et par conséquent de ne pas non plus avoir exigé davantage de précisions s'agissant de l'étendue spatiale du dispositif[1642]. Cependant, il convient de noter que le décret publié le 28 août 2023 portant sur l'article 10 de la loi JOP2024 est venu préciser les types d'évènements prédéterminés susceptibles de faire l'objet d'une analyse

---

[1637] CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.*, p. 1 : « Le projet de loi comprend plusieurs mesures, concernant divers domaines, nécessaires à l'organisation des jeux. […] Nombre de ces mesures ont un caractère permanent et sont conçues pour s'appliquer y compris en dehors de la période des jeux Olympiques et Paralympiques. Ainsi, si huit articles ne sont applicables qu'aux prochains jeux Olympiques et Paralympiques de 2024, dont deux ont un caractère expérimental, onze autres articles créent des dispositions nouvelles ou modifient des dispositions existantes de façon pérenne et seront donc susceptibles de s'appliquer à d'autres situations. Le Conseil d'État propose en conséquence de modifier le titre du projet de loi et de l'intituler comme "relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres propositions" ».

[1638] Excédant très largement la seule durée des évènements liés à la Coupe du monde de rugby de 2023 et les JOP de 2024.

[1639] À noter que la date de fin des expérimentations était initialement prévue pour le 30 juin 2025 (Sénat, Texte n° 220 sur le projet de loi (procédure accélérée) relatif aux jeux Olympiques et Paralympiques de 2024, art. 7 I [en ligne]) puis avait été modifiée, de manière plus cohérente, au 31 décembre 2024 (AN, Texte n°939, adopté par la commission, sur le projet de loi, adopté par le Sénat relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 9 mars 2023, art. 7 I [en ligne]) pour finalement être fixée par le texte publié au 31 mars 2025 sans préciser les raisons de son extension (Rapport législatif n° 496 de la Commission mixte paritaire, Projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, Compte-rendu intégral des débats du 4 avril 2023, art. 7 I [en ligne]). Ce report de la date finale de l'expérimentation était notamment contesté par les députés ayant effectué le dépôt du texte pour examen de conformité par le Conseil constitutionnel (C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.*, cons. 27).

[1640] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.*, cons. 47 : « en prévoyant que l'expérimentation autorisée par ces dispositions, qui n'a pas au demeurant pour objet de s'appliquer uniquement aux jeux olympiques et paralympiques de 2024, s'achèvera le 31 mars 2025, le législateur a précisément fixé la durée maximale de l'expérimentation qu'il a autorisée ».

[1641] *Idem*, cons. 37 : « les traitements algorithmiques des images ainsi collectées ne peuvent être mis en œuvre qu'afin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui […] sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes » et que par conséquent les dispositions sont suffisamment précises puisqu'elles limitent « l'usage de tels traitements à des manifestations présentant des risques particuliers d'atteintes graves à l'ordre public ».

[1642] Cette expérimentation ne se limite ni à la durée ni aux lieux où se dérouleront les JOP et par conséquent pourra être mise en œuvre lors de différentes manifestations sportives, récréatives ou culturelles (Loi JOP2024, art. 10 I.).

d'images par des caméras « augmentées »[1643]. En outre, et à l'instar de sa décision relative à l'examen de la loi RPSI s'agissant de l'emploi de caméras aéroportées[1644], le Conseil constitutionnel n'a exercé son examen de conformité qu'au regard du seul droit à la vie privée, les requérants n'ayant pas soulevé d'autres droits et libertés pouvant faire l'objet d'une restriction disproportionnée telle que la liberté d'aller et venir.

594. Néanmoins, le Conseil constitutionnel a émis une réserve d'interprétation obligeant le préfet « à mettre fin immédiatement à une autorisation [de recourir à une caméra « augmentée »] dont les conditions ayant justifié la délivrance ne sont plus réunies »[1645] sans possibilité d'éventuelle suspension[1646]. Il convient aussi de saluer l'initiative du Conseil constitutionnel qui s'est montré prudent et prévenant en énonçant déjà les conditions qu'il exigerait si un tel dispositif devait être pérennisé. Dans le cas où un texte devait lui être soumis ultérieurement par le législateur afin d'inscrire dans le droit commun de telles pratiques, les Sages ont de fait envisagé d'effectuer une analyse approfondie du rapport d'évaluation de cette expérimentation, particulièrement s'agissant de l'incidence sur le droit à la vie privée[1647].

595. Au regard de ce qui précède, le statut de garant de la protection des droits et libertés habituellement attribué au juge constitutionnel apparaît quelque peu discutable[1648]. Il semblerait que, face à la demande sociale, le Conseil constitutionnel ne puisse plus se permettre de s'élever contre les « évolutions juridiques et technologiques en matière de sécurité »[1649]. Cependant, il n'est pas le seul organe juridictionnel compétent pour assurer la protection des droits et libertés. Ainsi, si le Conseil constitutionnel a régulièrement exercé ses pouvoirs de contrôle de constitutionnalité sur les dispositions relatives à la sécurité publique, les juges ordinaires administratifs et judiciaires se

---

[1643] Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.*, art. 3.

[1644] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 46.

[1645] *Idem*, cons. 39.

[1646] Loi JOP2024, art. 10 VIII.

[1647] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit*., cons. 48.

[1648] À titre d'exemple, la décision rendue le 15 octobre 2021 par le juge constitutionnel surprend et laisse craindre un affaiblissement de la protection des droits et libertés lorsqu'il refuse au droit à la sûreté le statut de règle ou de principe inhérent à l'identité constitutionnelle de la France (C. const., Décision n° 2021-940 QPC, 15 octobre 2021, *op. cit.*, cons. 14).

[1649] LATOUR (X.), « Sécurité intérieure : un droit "augmenté" », *op. cit.*

sont également démarqués dans leur contrôle des mesures de police restrictives des droits et libertés, notamment celles portant sur le recours à des technologies de surveillance de sécurité publique.

§2. Les rôles du juge judiciaire et du juge administratif face aux technologies de surveillance de sécurité publique

596. La Constitution de 1958 attribue au juge judiciaire les compétences pour assurer la protection des droits et libertés. Ainsi, l'autorité judiciaire est reconnue comme la gardienne de la liberté individuelle[1650]. Ce principe est repris par le code de procédure pénale énonçant que « les mesures de contraintes dont [la personne suspectée ou poursuivie] peut faire l'objet sont prises sur décision ou sous le contrôle effectif de l'autorité judiciaire »[1651]. Depuis la révision des contours de la notion de liberté individuelle par le juge constitutionnel (v. **n° 526 et suiv.**), les compétences du juge judiciaire ont été limitées aux seules privations de libertés et aux détentions arbitraires[1652]. Au pénal, le juge judiciaire exerce son pouvoir juridictionnel sur les atteintes portées aux droits et libertés[1653]. À cette fin, il peut mettre en œuvre différentes procédures visant à faire cesser immédiatement une atteinte à un droit[1654] (A).

597. Le juge judiciaire ne détient pas le monopole de la protection des droits et libertés. Ainsi, tout acte impliquant une restriction des libertés individuelles et non une privation de celles-ci peut relever de la compétence soit du juge administratif soit du juge judiciaire. En ce sens, le doyen Jean Rivero avait déclaré que s'agissant de la protection des droits et libertés « les deux juridictions,

---

[1650] Constitution de 1958, art. 66 : « l'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe [nul ne peut être arbitrairement détenu] dans les conditions prévues par la loi » ; C. const., Décision n° 2004-492 DC, 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité, op. cit.* ; C. const., Décision n° 2010-14/22 QPC, 30 juillet 2010, *M. Daniel W. et autres*, *op. cit.*
Par ailleurs, l'article 5 de la Conv.EDH exige l'intervention de l'autorité judiciaire lorsqu'une personne est privée de liberté. Toutefois, il convient de noter que, bien que la Constitution n'en fasse pas mention, le juge administratif dispose également de compétences en matière d'atteinte à la liberté individuelle (HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 261 : « le juge administratif […] peut également être compétent vis-à-vis de mesures qui affectent la liberté individuelle ») et qu'il joue même un rôle « tout aussi essentiel […] s'agissant tout particulièrement du droit à la sûreté » (GARIDO (L.), « Le défenseur des droits, un progrès pour la protection du droit à la sûreté ? », p. 110 in GARRIDO (L.) (dir.), *Le droit à la sûreté : État des lieux, état du droit*, *op. cit.*).

[1651] CPP, art. Préliminaire, al. 7.

[1652] PERERA (S.), *Le principe de liberté en droit public français*, *op. cit.*, p. 163.

[1653] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 113.

[1654] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 293.

chacune selon sa spécialité, ont mis des moyens différents mais complémentaires : le juge administratif a situé l'essentiel de son action au niveau des normes, le juge judiciaire au niveau des réalités concrètes »[1655]. De même, l'article 61-1 de la Constitution attribue tant au juge judiciaire qu'au juge administratif la possibilité de transmettre une question prioritaire de constitutionnalité au juge constitutionnel afin d'assurer la protection des droits et libertés[1656]. Dès lors, le juge administratif joue un rôle essentiel, principalement au moyen du référé-liberté introduit par la loi du 30 juin 2000[1657] et notamment en rappelant l'exigence de publication des mesures de police restrictives des libertés publiques[1658]. C'est dans le cadre de cette procédure qu'il a eu à rendre des décisions portant sur le recours à des drones aériens de sécurité publique (B).

A. La protection du juge judiciaire à l'ère des technologies de surveillance de sécurité publique

598. Le Tribunal des conflits avait déjà jugé en 1947 dans sa décision *Hilaire*, que « la sauvegarde de la liberté individuelle rentre essentiellement dans les attributions de l'autorité judiciaire »[1659]. Aussi, le juge constitutionnel attribue au juge judiciaire la compétence exclusive en matière de contentieux liés spécifiquement à la détention[1660]. Le code de procédure pénale précise ainsi que « dans tous les cas d'atteinte à la liberté individuelle, le conflit ne peut jamais être élevé par l'autorité administrative et les tribunaux de l'ordre judiciaire sont toujours exclusivement compétents »[1661]. Le principe d'exclusivité du contentieux relatif à la protection de la liberté

[1655] RIVERO (J.), « Dualité de juridictions et protection des libertés », *RFDA*, 1990, p. 736.

[1656] Depuis la révision constitutionnelle de la loi du 23 juillet 2008, l'article 61-1 de la Constitution dispose que « lorsque, à l'occasion d'un litige en cours devant une juridiction, il est soutenu qu'une disposition législative porte atteinte aux droits et libertés que la Constitution garantit, le Conseil constitutionnel peut être saisi de cette question sur renvoi du Conseil d'État ou de la Cour de cassation qui se prononce dans un délai déterminé ». Voir notamment : DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 30 ; GRANGER (M-A.), « La sécurité publique sous contrôle juridictionnel : polices et autorité judiciaire dans la jurisprudence constitutionnelle depuis la décision Fouille de véhicules de 1977 », pp. 41-51, *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2022 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, vol. 7, 2022, 316 p., p. 43.

[1657] Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives, *JORF* n°151 du 1 juillet 2000 [en ligne] inscrite dans le Code de justice administrative (CJA), spéc. art. L. 521-1 et L. 521-2.

[1658] TA Paris, ord., 4 avril 2023, n° 2307385/9, *Association défense des libertés constitutionnelles et a.* [en ligne] : « Sauf motif impératif d'urgence lié au maintien et la sauvegarde de la sécurité publique dans une situation grave, une mesure de police restreignant les libertés publiques doit être publiée dans un délai permettant un accès utile au juge des référés saisi sur le fondement de l'article L. 521-2 du code de justice administrative ».

[1659] TC, 18 décembre 1947, *Hilaire*, Rec. CE p. 516.

[1660] ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, *op. cit.*, p. 76.

[1661] CPP, art. 136, al. 3

individuelle au juge judiciaire a été affirmé par le Conseil constitutionnel dans sa décision de 1999[1662] lorsqu'il a restreint le champ de cette liberté (v. **n° 526**). Dès lors, le juge constitutionnel reconnait aux membres de l'autorité judiciaire un devoir d'intervention quand toute personne est sujette à une privation de liberté[1663]. Aussi, il vérifie que l'autorité judiciaire assure un contrôle effectif et permanent de la privation de liberté[1664]. Ainsi, l'autorité judiciaire assure un contrôle sur les forces de police judiciaire et garantit une protection des droits et libertés des personnes suspectées ou poursuivies notamment au moyen des principes de nécessité et de proportionnalité[1665]. En ce sens, la Cour de cassation n'a pas hésité à mentionner le droit à la sûreté, considérant qu'il « commande au juge pénal, lorsqu'il envisage, dans un cas prévu par la loi, de prononcer une peine privative de liberté à l'encontre d'une personne poursuivie au seul motif qu'elle s'est soustraite à l'exécution d'un acte administratif la concernant, de s'assurer préalablement que l'obligation dont la violation est alléguée était nécessaire et proportionnée »[1666].

599. Le juge judiciaire est également compétent pour sanctionner les atteintes à certains droits et libertés, y compris celles résultant d'agents de l'État[1667], que sont la liberté individuelle[1668], la non-discrimination[1669], l'inviolabilité du domicile[1670] et le secret des correspondances[1671] (ces deux derniers étant des composantes du droit à la vie privée). Il peut mettre en œuvre différentes procédures de référé afin de faire cesser les atteintes à un de ces droits[1672]. En premier lieu, le juge judiciaire dispose d'un référé de droit commun qui lui permet de « prescrire en référé les mesures

---

[1662] C. const., Décision n° 99-411 DC, 16 juin 1999, *op. cit.* ; C. const., Décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, *op. cit.*

[1663] C. const., Décisions n° 93-326 DC, 11 août 1993, *Loi modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme du code de procédure pénale*, Rec. p. 217, cons. 5 [en ligne] ; C. const., Décision n° 2010-14/22 QPC, 30 juillet 2010, *op. cit.*, cons. 26.

[1664] GRANGER (M-A.), « La sécurité publique sous le contrôle juridictionnel : polices et autorité judiciaire dans la jurisprudence constitutionnelle depuis la décision Fouille de véhicules de 1977 », in GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2022 Du droit de la sécurité et de la défens*e, op. cit., pp. 41-51, spéc. p. 45.

[1665] CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, *op. cit.*, spéc. pp. 696-700.

[1666] C. cass., ch. crim., 3 mai 2017, n° 16-86.155 [en ligne].

[1667] GRANGER (M-A.), « La sécurité publique sous le contrôle juridictionnel : polices et autorité judiciaire dans la jurisprudence constitutionnelle depuis la décision Fouille de véhicules de 1977 », in GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2022 Du droit de la sécurité et de la défens*e, op. cit., pp. 41-51, spéc. p. 46.

[1668] CP, art. 432-4 à 432-6.

[1669] CP, art. 432-7.

[1670] CP, art. 432-8.

[1671] CP, art. 342-9

[1672] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, pp. 293-295.

conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite »[1673]. À titre d'exemple, il a pu rendre des décisions en référé portant notamment sur le droit à la non-discrimination[1674]. En deuxième lieu, il peut mettre en œuvre d'autres procédures plus spécifiques de référé. Ainsi, le juge judiciaire garantit une protection au droit à la vie privée sur le fondement de l'article 9 du Code civil énonçant que « les juges peuvent […] prescrire toutes mesures […] propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé »[1675]. Cette procédure est conditionnée par une démonstration par le requérant d'une atteinte à sa vie privée et du caractère d'urgence[1676]. Le juge judiciaire est également compétent pour prendre des mesures en référé en matière de présomption d'innocence sur le fondement de l'article 9-1 du Code civil qui dispose qu'il peut « prescrire toutes mesures […] aux fins de faire cesser l'atteinte à la présomption d'innocence, et ce aux frais de la personne, physique ou morale, responsable de cette atteinte »[1677]. L'application de cette mesure de référé est soumise à la seule condition de démonstration de la méconnaissance de la présomption d'innocence[1678].

600. Dans le cadre des atteintes à la liberté individuelle, le juge judiciaire examine l'admissibilité des preuves qui ont servi à la privation de liberté ou à la mise en détention. Pour rappel, les preuves au moyen de systèmes de vidéoprotection sont admises par le juge judiciaire[1679] (v. **n° 465 et suiv.**). Dès lors, les images collectées par les drones aériens de sécurité publique pourraient être recevables à titre de preuve sous réserve de répondre aux exigences de légalité et de ne pas avoir été altérées. Le juge judiciaire pourrait donc prochainement être amené à traiter d'affaires portant sur des infractions filmées par des drones aériens de sécurité publique. Pour l'heure, la Cour de cassation n'a été saisie que d'une affaire portant sur l'emploi de drones aériens à des fins d'enquête judiciaire pour filmer le domicile d'une personne suspectée de participer à un

---

[1673] Code de procédure civile (CPC), art. 835, al. 1er.

[1674] C. cass., ch. soc., 18 février 2014, n° 13-10.294 [en ligne].

[1675] C. civ., art. 9.

[1676] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 294.

[1677] C. civ., art. 9-1, al. 2.

[1678] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, pp. 294-295.

[1679] C. cass., 27 novembre 2002, n° 02-80-659 [en ligne] ; C. cass., 31 mai 2005, n° 04-85-469 [en ligne]. Voir aussi : MORNET (M-N.), *La vidéosurveillance et la preuve, op. cit.*

trafic de stupéfiants[1680] (v. **n° 847**). Le juge judiciaire dispose donc d'un rôle essentiel en matière de contrôle des technologies de surveillance de sécurité publique bien qu'il n'agisse essentiellement qu'en matière d'atteinte à la liberté individuelle. Le juge administratif a, pour sa part, déjà rendu plusieurs décisions concernant le recours à des drones aériens de sécurité publique, notamment dans le cadre de procédures en référé-liberté.

B. Le juge administratif, premier protecteur des droits et libertés à l'ère des technologies de surveillance de sécurité publique ?

601. Le juge administratif assure le contrôle de la légalité des actions des pouvoirs publics et, de ce fait, endosse un rôle fondamental garantissant le respect des droits et libertés[1681], notamment face aux décisions arbitraires et aux abus de pouvoir[1682]. Cependant, la conception restrictive de la liberté individuelle par le juge constitutionnel depuis 1999 attribuant l'unique compétence au juge judiciaire (v. **n° 526 et suiv.**), d'une part, et la conception extensive de la police administrative, d'autre part, ont réduit les possibilités de garantir la protection effective des droits et libertés en faisant peser la majeure partie du contrôle sur le juge administratif[1683]. De fait, ses compétences n'ont eu de cesse de s'étendre en matière de protection des droits et libertés[1684]. Or, les compétences attribuées au juge administratif qui relevaient auparavant de la compétence du juge judiciaire ont eu pour effet de mettre en concurrence les deux juridictions[1685]. En outre, la politique sécuritaire mise en œuvre depuis le début des années 2000 s'est appuyée sur cette nouvelle répartition des

---

[1680] C. cass., ch. crim., 15 novembre 2022, n° 22-80-097, *op. cit.*

[1681] En ce sens, le professeur René Chapus considérait que les libertés fondamentales dégagées par le juge administratif l'avait progressivement transformé en une véritable « juridiction des droits de l'homme » (CHAPUS (R.), *L'administration et son juge*, Paris, PUF, 1999, 426 p., p. 15). À noter que les libertés fondamentales sur lesquelles se fonde le juge administratif diffèrent et sont plus nombreuses que celles dégagées par le juge constitutionnel (DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, pp. 122-123).

[1682] SAUVÉ (J-M.), « Le juge administratif et les droits fondamentaux », *AJDA* n° 43, 19 décembre 2016, p. 2420 ; SIZAIRE (V.), « Le juge administratif et la protection des libertés. Éléments pour une garde partagée », *RDLF*, 2019, chron. n° 27.

[1683] LATOUR (X.), « Sécurité intérieure : un droit "augmenté" », *op. cit.* Voir aussi : LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *op. cit.* : « le juge administratif par une extension sans précédent des prérogatives de la police administrative acquiert des compétences nouvelles induisant une éviction du juge judiciaire ».

[1684] ANDRIANTSIMBAZOVINA (J.), « La protection des libertés, fondement de la compétence du juge administratif ? », *RGD*, chron. « Doits des libertés », 2019. Voir aussi : PACTEAU (B.), « Justice administrative », *in* ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, *op. cit.*

[1685] SIZAIRE (V.), « Le juge administratif et la protection des libertés. Éléments pour une garde partagée », *op. cit.*

compétences juridictionnelles afin de « contourner les garanties offertes par la procédure pénale »[1686].

602. Le rôle de garant du juge administratif repose aussi sur une extension du contrôle qu'il exerce sur les mesures administratives les plus attentatoires aux droits et libertés[1687], d'une part, et par l'introduction de la procédure de référé par la loi du 30 juin 2000[1688], d'autre part[1689]. Cette procédure lui a permis de devenir le « juge de l'urgence »[1690] lorsqu'une atteinte grave est portée aux droits et libertés reconnus comme fondamentaux[1691]. De fait, les procédures de référés administratifs, telles que le référé suspension[1692] ou le référé liberté[1693], sont une garantie capitale offertes par le juge administratif permettant de répondre, dans les plus brefs délais, aux atteintes les plus graves aux droits et libertés[1694]. Ces procédures sont, cependant, soumises à la condition que le

---

[1686] *Ibid*.

[1687] ANDRIANTSIMBAZOVINA (J.), « La protection des libertés, fondement de la compétence du juge administratif ? », *op. cit.*, pp. 5-6 : « le juge administratif a l'obligation de garantir aux justiciables le contrôle juridictionnel des actes pris par l'administration dans l'exercice des prérogatives de puissance publique et la protection substantielle des libertés des justiciables ».

[1688] Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives, *JORF* n°151 du 1 juillet 2000 [en ligne].

[1689] SIZAIRE (V.), « Le juge administratif et la protection des libertés. Éléments pour une garde partagée », *op. cit.*

[1690] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 121.

[1691] STIRN (B.), « Ordre public et libertés publiques », *in* SÈVE (R.), *L'ordre public*, *op. cit.*, pp. 5-15, spéc. p. 12 : « l'urgence se manifeste surtout par des procédures qui donnent au contrôle du juge sa pleine effectivité. Dans le développement des procédures d'urgence, le droit des libertés occupe en effet une place particulière ».

[1692] CJA, art. L. 521-1 : « Quand une décision administrative, même de rejet, fait l'objet d'une requête en annulation ou en réformation, le juge des référés, saisi d'une demande en ce sens, peut ordonner la suspension de l'exécution de cette décision, ou de certains de ses effets, lorsque l'urgence le justifie et qu'il est fait état d'un moyen propre à créer, en l'état de l'instruction, un doute sérieux quant à la légalité de la décision ».

[1693] CJA, art. L. 521-2 : « Saisi d'une demande en ce sens justifiée par l'urgence, le juge des référés peut ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle une personne morale de droit public ou un organisme de droit privé chargé de la gestion d'un service public aurait porté, dans l'exercice d'un de ses pouvoirs, une atteinte grave et manifestement illégale. Le juge des référés se prononce dans un délai de quarante-huit heures ».

[1694] STIRN (B.), « Ordre public et libertés publiques », *in* SÈVE (R.), *L'ordre public*, *op. cit.*, pp. 5-15, spéc. p. 13 : « Par la généralité de son champ, la brièveté des délais, l'étendue des pouvoirs conférés au juge, le référé-liberté constitue une procédure particulièrement efficace ». L'auteur ajoute que « le référé [suspension ou liberté] a donné aux recours devant le juge administratif une effectivité fortement accrue ». ANDRIANTSIMBAZOVINA (J.), « La protection des libertés, fondement de la compétence du juge administratif ? », *op. cit.*, p. 11 : « À travers le recours pour excès de pouvoir, la doctrine universitaire prête également au juge administratif une fonction importante de protection des libertés ».

justiciable soit en mesure de démontrer le caractère urgent de sa requête[1695].

603. Le succès de la procédure de référé-liberté[1696] s'est globalement confirmé concernant le contentieux lié au recours à des drones aériens par les forces de l'ordre (1). Aussi, le juge administratif n'est pas uniquement compétent au contentieux et formule également des recommandations sur des sujets d'actualités ou encore des avis concernant un texte législatif en cours d'élaboration, qui peuvent avoir une influence sur les décisions du législateur ou sur le comportement des personnes[1697]. Dans le cadre du projet de loi JOP2024, il a ainsi rendu un avis concernant notamment les dispositions relatives à l'emploi de caméras « augmentées » à des fins de sécurité publique (2).

1. Le référé-liberté, une garantie des droits et libertés du juge administratif : l'exemple des drones aériens de sécurité publique

604. Les arrêts rendus par le Conseil d'État concernant le recours à des drones aériens de surveillance par la Préfecture de Police de Paris lors de la crise sanitaire du Covid-19 au printemps et à l'automne 2020[1698] tendent à confirmer le rôle de protecteur des droits et libertés attribué au juge administratif (v. **n° 183-188**). Ils démontrent de manière éloquente que le Conseil d'État peut parfois se révéler plus protecteur des droits et libertés que ne l'est le Conseil constitutionnel. En ce sens, Olivier Schrameck reprochait au juge constitutionnel d'exécuter de manière incertaine son rôle d'assurer la compatibilité entre les libertés et l'ordre public[1699]. Ainsi, il affirmait que le juge constitutionnel laissait « plus ou moins de latitude au législateur jusqu'à se contenter de relever que

---

[1695] SIZAIRE (V.), « Le juge administratif et la protection des libertés. Éléments pour une garde partagée », *op. cit.* Voir notamment : CE, ord., 19 décembre 2012, n° 364444 [en ligne] : « L'usage par le juge des référés, des pouvoirs qu'il tient des dispositions de l'article L. 521-2 du code de justice administrative est subordonné à la condition qu'une urgence particulière rende nécessaire l'intervention à très brève échéance d'une décision destinée à la sauvegarde d'une liberté fondamentale ».

[1696] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 288 : « Le référé-liberté est rapidement devenu un outil essentiel de la garantie des libertés et des droits fondamentaux à l'égard de l'administration ».

[1697] SAUVÉ (J-M.), « le juge administratif et les droits fondamentaux », *op. cit.*

[1698] CE, ord., 18 mai 2020, n°440442, *op. cit.* et CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155, *op. cit.*

[1699] SCHRAMECK (O.), « Sécurité et libertés », *RFDA*, 2011, p. 1093.

celui-ci a assuré une conciliation qui "n'est pas manifestement disproportionnée"[1700], alors que, pour sa part, le Conseil d'État persiste à exiger une stricte proportionnalité en matière de police administrative »[1701].

605. Lors des deux saisines du Tribunal administratif de Paris par l'association *La Quadrature du Net* et la Ligue des droits de l'homme concernant le recours à des drones aériens par les forces de l'ordre en 2020 au motif d'une atteinte au droit à la vie privée et à la protection des DACP, les premiers juges avaient rejeté les demandes en référé. Dans la première affaire, les requérants s'étaient opposés à l'usage de drones aériens par les forces de l'ordre pour faire respecter les mesures de confinement mais avaient été déboutés par le Tribunal administratif de Paris au motif que les données collectées ne constituaient pas des DACP[1702]. Portant leur affaire devant le Conseil d'État, celui-ci avait abondé dans le sens des demandeurs estimant que les données collectées entraient dans le cadre de la réglementation relative à la protection des DACP dans la mesure où le zoom utilisé et le vol en basse altitude ne permettaient pas de rendre « impossible l'identification des personnes filmées »[1703]. Dès lors, il avait souligné l'absence de texte réglementaire préalable autorisant leur mise en œuvre et donc la violation de l'article 31 de la LIL[1704]. Si le Conseil d'État avait considéré que les techniques employées ne permettaient pas d'assurer le respect du droit à la vie privée, il ne s'était néanmoins pas opposé sur le principe au recours à cette technologie par les forces de l'ordre[1705].

606. Dans la deuxième affaire, les requérants alléguaient que les images collectées par les drones aériens de sécurité publique à des fins de surveillance des manifestations comprenaient des

---

[1700] Voir : C. const., Décision n° 2010-613 DC, 7 octobre 2010, *Loi interdisant la dissimulation du visage dans l'espace public*, *op. cit.* ; C. const., Décision n° 2015-713 DC, 23 juillet 2015, *Loi relative au renseignement*, *JORF* n°0171 du 26 juillet 2015 page 12751, texte n° 4 [en ligne] ; C. const., Décision n° 2015-722 DC, 26 novembre 2015, *Loi relative aux mesures de surveillance des communications électroniques internationales*, *JORF* n°0278 du 1 décembre 2015 page 22187, texte n° 2 [en ligne].

[1701] SCHRAMECK (O.), « Sécurité et libertés », *op. cit.*

[1702] TA Paris, ord., 5 mai 2020, n°2006861/9, *op. cit.*

[1703] CE, ord., 18 mai 2020, n°440442, *op. cit.*, cons. 19.

[1704] *Idem*, cons. 18.

[1705] *Idem*, cons. 13.

DACP, y compris des données sensibles[1706] au sens de la règlementation[1707]. Cependant, les juges du fond avaient estimé que la décision du ministère de l'Intérieur d'avoir recours à des drones aériens afin de surveiller les manifestations n'était « entachée » d'aucun « doute sérieux quant à sa légalité » considérant que les mesures de floutage qui avaient été intégrées étaient un « obstacle suffisant à toute identification »[1708]. Les requérants avaient alors saisi le Conseil d'État qui avait de nouveau donné raison à *La Quadrature du Net* dans un arrêt rendu le 22 décembre 2020[1709]. À cette occasion, il avait une fois encore annulé l'ordonnance du Tribunal administratif de Paris du 4 novembre 2020 au motif qu'en dépit du floutage des images des manifestants collectées par les drones aériens, les données identifiantes faisaient au préalable l'objet d'un traitement par le logiciel permettant le floutage et qu'il s'agissait donc d'un traitement de DACP au sens de la DPJ[1710]. Le Conseil d'État avait une nouvelle fois soulevé l'illégalité de la mesure en raison de l'absence de texte réglementaire autorisant leur recours[1711].

607. Ainsi, le Conseil d'État s'est montré très protecteur des droits et libertés face à l'emploi de drones aériens de sécurité publique avant qu'ils soient encadrés par la loi RPSI. Par la suite, le juge administratif s'est rangé derrière la position du Conseil constitutionnel pour juger la demande (encore au moyen d'un référé-liberté) de suspension du décret du 19 avril 2023 d'application de la loi RPSI portant sur l'usage de drones aériens par les forces de l'ordre[1712] dans une décision du 24 mai 2023[1713]. Les requérants avaient contesté la légalité du décret invoquant pas moins de neuf motifs. Le Conseil d'État avait rappelé que le respect de l'ensemble des dispositions législatives et réglementaires en matière de recours à des drones aériens par les forces de l'ordre « s'apprécie décision d'autorisation par décision d'autorisation, que les intéressés […] peuvent contester devant

---

[1706] RGPD, art. 9 ; DPJ, art. 10 ; LIL, art. 6.

[1707] Le « Schéma national du maintien de l'ordre », publié par le ministère de l'Intérieur le 16 septembre 2020 [en ligne], mentionnait effectivement que les drones aériens étaient équipés de « capteurs optiques et de capacités de retransmission » (art. 3.4.2) et qu'ils avaient notamment pour finalités « l'identification des auteurs d'éventuelles exactions et comportements violents » (art. 3.2.1 et art. 3.2.4).

[1708] TA Paris, ord., 4 novembre 2020, n° 2017540/3/5 [en ligne].

[1709] CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155, *op. cit.*, cons. 13.

[1710] *Idem*, cons. 8.

[1711] *Idem*, cons. 13.

[1712] Décret n° 2023-283 du 19 avril 2023 relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs pour des missions de police administrative, *op. cit.*

[1713] CE, ord., 24 mai 2023, n° 473547, *M. B... et l'Association de défense des libertés constitutionnelles* [en ligne].

le juge de l'excès de pouvoir en assortissant, en cas d'urgence, leur demande d'annulation d'une demande de suspension de leur exécution adressée au juge des référés »[1714].

608. D'une manière générale, la décision de rejet de la requête du juge administratif ne surprend pas et se révèle plutôt cohérente. Cependant, il paraît regrettable que les dispositions du décret contesté relatives à l'information de leur usage n'aient pas fait l'objet d'un contrôle plus strict de la part du Conseil d'État. Ainsi, l'un des motifs dénonçait la méconnaissance du droit à l'information du public et du droit au respect à la vie privée résultant de l'absence de détail des « modalités de mise en œuvre de l'information des personnes filmées et du public » et de précision des « circonstances justifiant qu'il soit dérogé au principe d'information du public »[1715]. À cela, le juge administratif avait estimé que les notions de « public » et de « *moyen approprié* » ne nécessitaient pas « de précision de la part du pouvoir réglementaire, quand bien même, sur ce point également, les doctrines d'emploi élaborées par chaque ministère pourront utilement détailler les modalités opérationnelles envisageables »[1716]. Il avait notamment ajouté que la demande d'autorisation préalable devait préciser « le cas échéant, les modalités d'information du public »[1717] et que l'autorité délivrant l'autorisation devait « justifier du caractère approprié, au regard de la configuration de chaque espèce, des moyens d'information du public employés »[1718]. Il aurait été souhaitable que le juge administratif exige davantage de précisions concernant les modes concrets de mise en œuvre du droit à l'information du public compte tenu du fait que les suggestions formulées par la CNIL dans son avis sur le décret contesté n'avaient pas été prises en compte[1719].

2. Les recommandations du Conseil d'État en matière de technologies « augmentées » à des fins de sécurité publique

609. Dans son avis portant sur le projet de loi JOP2024, le Conseil d'État avait formulé quelques recommandations s'agissant de l'emploi de caméras de vidéoprotection « augmentées »

[1714] *Idem*, cons. 8.

[1715] *Idem*, dernier motif formulé par les premiers requérants (M. B... et l'Association de défense des libertés constitutionnelles).

[1716] *Idem*, cons. 17.

[1717] CSI, art. L. 242-5, 6°).

[1718] CE, ord., 24 mai 2023, n° 473547, *op. cit.*, cons. 17.

[1719] CNIL, Délibération n° 2023-027 du 16 mars 2023, *op. cit.*

notamment à des fins de surveillance des évènements liés aux JOP qui se dérouleront à Paris durant l'été 2024[1720]. Le Conseil d'État, tenant compte des besoins requis par les forces de l'ordre à l'avènement des JOP de Paris 2024, avait reconnu la légitimité des autorités publiques de vouloir mettre en œuvre des dispositifs de vidéoprotection associés à des algorithmes d'analyse d'images afin de pallier les limites quant aux « capacités d'attention et d'analyse humaines mobilisables »[1721]. À cet effet, il avait admis la nécessité d'adopter un cadre législatif temporaire pour encadrer ces usages compte tenu de l'absence de cadre légal propre aux SIA. Le Conseil d'État avait ensuite fait une description des phases de contrôle de l'algorithme d'analyse d'images de sa conception à son usage. Ainsi, il est intéressant de remarquer qu'il ne s'oppose pas à ce que le traitement puisse être opéré par un prestataire extérieur[1722] sans préciser si celui-ci relèvera du droit de l'Union européenne en matière de protection des DACP ou non. De fait, le Conseil d'État se révèle beaucoup plus vigilant dans les recommandations issues de son étude portant sur l'IA[1723]. Par ailleurs, il convient de noter qu'il avait proposé de repousser la durée de l'expérimentation des caméras de vidéoprotection « augmentées » à juin 2025[1724], en d'autres termes, près d'un an après la fin des JOP 2024 prétextant que cela servirait au rapport d'évaluation transmis au Parlement et à la CNIL. Les dispositions relatives aux usages expérimentaux de la loi JOP2024 n'ont finalement été prolongées qu'au mois de mars 2025[1725].

610. Conclusion - Le juge administratif se pose en protecteur des droits et libertés par sa procédure de référé, principalement celle de référé-liberté, qui lui permet de se prononcer dans un bref délai et de faire face aux enjeux d'actualité. Ainsi, cette procédure « donne à la juridiction administrative non seulement une grande efficacité mais aussi une visibilité accrue dans son rôle de défense des libertés »[1726]. Si le juge administratif a démontré en de nombreuses occasions qu'il était un réel défenseur des droits et libertés, certaines de ses décisions viennent contredire cette position

---

[1720] CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 15 décembre 2022, *op. cit.*

[1721] *Idem*, §23.

[1722] *Idem*, §25.

[1723] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, spéc. pp. 130-134.

[1724] CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 15 décembre 2022, *op. cit.,* §26.

[1725] Loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.*, art. 10, I.

[1726] STIRN (B.), « Ordre public et libertés publiques », *in* SÈVE (R.), *L'ordre public*, *op. cit.*, pp. 5-15, spéc. p. 14.

notamment s'agissant des mesures de collecte indifférenciée de DACP à des fins de surveillance dans un cadre de sécurité nationale dans l'arrêt *French Data Network et a.* du 21 avril 2021[1727]. Cette décision tend à confirmer la position des détracteurs du juge administratif qui critiquent sa protection insuffisante des droits et libertés[1728] en assurant un simple « contrôle de la conciliation faite par l'administration, notamment dans l'exercice de son pouvoir de police, entre les libertés des particuliers et la sauvegarde de l'ordre public »[1729]. En outre, le Conseil d'État semble moins opposé à la surveillance de masse que ne l'est la CJUE, notamment dans son arrêt *La Quadrature du Net et a.* du 6 octobre 2020[1730]. L'exemple de ces affaires dénote des divergences sensibles entre la juridiction nationale et la juridiction européenne qui entachent la protection des droits et libertés.

Section 2 L'insuffisance des garanties face aux technologies de surveillance de sécurité publique

611. Lorsque la protection des droits et libertés fait défaut face aux juridictions nationales, les juridictions européennes se présentent souvent comme des garants de choix, en dépit du fait qu'elles ne puissent être saisies qu'après épuisement des recours en interne, en application du principe de subsidiarité, ou par voie de question préjudicielle (§1). Aussi, la protection non juridictionnelle des droits et libertés, principalement assurée par les AAI, constitue également une solution non négligeable. Néanmoins, la compétence croissante de ces autorités demeure insuffisante pour garantir de manière effective le respect des droits et libertés confrontés aux développements exponentiels des technologies de surveillance dont celles destinées à un usage de sécurité publique (§2).

[1727] CE, ass., 21 avril 2021, n° 393099, 394922, 397844, 397851, 424717, 424718, *French data Network et a., op. cit.*

[1728] Voir notamment : LOCHAK (D.), « Le juge administratif, protecteur des libertés », *in* Association française pour la recherche en droit administratif, *Les controverses en droit administratif*, Paris, Dalloz, 2017, 240 p., spéc. pp. 61-74.

[1729] ANDRIANTSIMBAZOVINA (J.), « La protection des libertés, fondement de la compétence du juge administratif ? », *op. cit.*, p. 13. Voir aussi : PLESSIX (B.), *Droit administratif général*, *op. cit.*, pp. 805-829.

[1730] CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.*

§1. La jurisprudence européenne, instrument de protection des droits et libertés

612. La jurisprudence émanant tant de la CEDH que de la CJUE est aussi importante[1731] qu'innovante, plus particulièrement lorsque les deux instances ont à traiter d'affaires portant sur les nouvelles technologies. En dépit du fait que leur approche diffère sensiblement, notamment s'agissant des affaires portant sur la surveillance de masse[1732], les deux juridictions européennes se sont, aujourd'hui, imposées en garantes des droits et libertés. Pourtant, si le juge des droits de l'homme a toujours eu pour fonction d'assurer le respect des dispositions de la Conv.EDH, le juge de l'Union européenne n'était pas originairement destiné à protéger les droits et libertés aujourd'hui inscrits dans la CDFUE[1733]. Cependant, la CJUE ne se prive pas de rendre ses décisions sur le fondement de la Charte des droits fondamentaux de l'Union européenne. Face au recours massif aux nouvelles technologies, et prochainement aux technologies « augmentées », au sein de la société, la CEDH (A) et la CJUE (B) ont déjà eu l'occasion de s'illustrer sur ce sujet notamment dans le cadre de plusieurs affaires portant sur l'emploi de technologies par les autorités publiques de différents États membres à des fins de surveillance.

A. Le rôle déclinant du juge européen des droits de l'homme face aux technologies de surveillance

613. Dans le cadre de ses fonctions visant à faire respecter les dispositions de la Conv.EDH, la CEDH s'est pleinement saisie de la question portant sur les conséquences des technologies sur les droits et libertés[1734] et notamment de celles utilisées par les autorités publiques. Leur usage à des

---

[1731] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 115 : « La Cour [européenne des droits de l'homme] fait l'objet d'un véritable engouement facilité par des conditions de recevabilité parfois libéralement interprétées » ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 128 : « depuis sa création en 1959, la Cour [européenne des droits de l'homme] a rendu plus de 22 500 arrêts ».

[1732] DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *RDP* n° 3, 1er mai 2022, p. 845.

[1733] En dépit du fait que la CJUE n'a pas initialement comme principale vocation la protection des droits et libertés (DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 156).

[1734] Voir sur le sujet : CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 20 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, pp. 316-324 ; ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, 2022, pp. 271-285. Voir aussi : LE BONNIEC (N.), « La Cour européenne des droits de l'homme face aux nouvelles technologies de l'information et de communication numériques », *RDLF* 2018, chron. n° 5 [en ligne].

fins de surveillance par un État a déjà fait l'objet de deux arrêts[1735] qui, pour en saisir le sens, nécessitent une analyse préalable des restrictions possibles aux droits et libertés à des fins de sauvegarde de l'ordre public (1). Aussi, les deux arrêts rendus en matière de surveillance de masse ainsi que ceux portant sur l'emploi d'algorithmes à des fins de prévention d'infractions permettent d'envisager les décisions futures de la CEDH en matière de technologies « augmentées » de surveillance de sécurité publique (2).

1. Le contrôle de la « clause d'ordre public » restrictive des droits et libertés dans la jurisprudence de la Cour européenne des droits de l'homme

614. La CEDH admet, en application de la Conv.EDH, une « marge nationale d'appréciation » permettant aux États parties de restreindre certains droits qu'elle énonce en vue de protéger la société démocratique et selon les circonstances[1736]. Ainsi, au sens de ce texte, l'ordre public constitue une condition spécifique permettant de justifier les restrictions aux droits et libertés[1737]. Or, la sécurité étant une composante de l'ordre public, celle-ci serait par conséquent constitutive d'une clause de restriction des droits et libertés ou, selon les termes de la Conv.EDH, d'une « clause d'ordre public »[1738]. Cette dernière permet de définir les conditions nécessaires à remplir afin que la mesure nationale restrictive soit compatible avec la Conv.EDH[1739]. Dans une décision du 6 septembre 1978, la CEDH a apporté des précisions concernant cette « clause d'ordre public », énonçant qu'elle n'est pas « une clause spécifique aux restrictions des droits mais bien au contraire une nécessité, une mesure de « sécurité-liberté », pour protéger la société démocratique dans son

---

[1735] CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, n° 35252/08 [en ligne] ; CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*

[1736] De manière non-exhaustive : SUDRE (F.), *La convention européenne des droits de l'Homme*, PUF, coll. Que sais-je ?, 11ème édition, 2021, 125 p., spéc. pp. 37-39 ; KISSANGOULA (J.), « La sécurité dans la jurisprudence de la CEDH », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 229-252, spéc. p. 247 ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *AJDA* n° 14, 19 avril 2021, p. 793 ; ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, spéc. p. 283 ; DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.*

[1737] Conv.EDH, art. 6 §2, 8 §2, 9 §2, 10 §2, 11 §2, 15 et 17 ; Protocole n° 4, art. 2 §3 ; Protocole n° 7, art. 1er §2.

[1738] À titre d'exemple des décisions portant sur la sécurité : CEDH, gr. ch., 6 septembre 1978, *Klass et autres c. Allemagne*, *op. cit.* ; CEDH, 2 août 1984, *Malone c. Royaume-Uni*, n° 8691/79 [en ligne] ; CEDH, gr. ch., 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06 [en ligne] ; CEDH, 13 avril 2017, *Tagayeva et autres c. Russie*, n° 26562/07 et 6 autres [en ligne].

[1739] SUDRE (F.), *Droit européen et international des droits de l'homme*, *op. cit.*, p. 207.

ensemble »[1740]. Ces conclusions s'inscrivent dans la logique de la position adoptée par la CEDH qui estime qu'étant « en contact direct et constant avec les réalités pressantes du moment, les autorités nationales se trouvent en principe mieux placées que le juge international pour se prononcer sur la présence de pareil danger comme sur la nature et l'étendue de dérogations nécessaires pour le conjurer »[1741].

615. Cependant, le pouvoir de restriction des droits et libertés laissé aux États parties en vue d'assurer la sauvegarde de l'ordre public n'est pas illimité et fait l'objet d'un examen par la CEDH européenne des droits de l'homme, qui dispose d'un pouvoir de contrôle de proportionnalité[1742] (v. **n° 821 et suiv.**). En d'autres termes, elle met en œuvre des limites aux restrictions des droits garantis par la Conv.EDH, permises par la marge d'appréciation des États. À cette fin, elle procède à un examen de la légitimité, de la légalité et de la nécessité de la mesure en cause[1743]. En d'autres termes, la CEDH effectue une analyse de la proportionnalité de « la clause d'ordre public » au regard de « la finalité de la mesure litigieuse et [de] sa "nécessité" dans une société démocratique »[1744]. En outre, la CEDH prévoit des conditions strictes s'agissant de l'application de l'article 15 de la Conv.EDH relative à l'état d'urgence[1745]. Pour autant, il apparait que la jurisprudence du juge européen des droits de l'homme tende à privilégier la « marge nationale

---

[1740] CEDH, gr. ch., 6 septembre 1978, *Klass et autres c. Allemagne*, *op. cit.*, §59.

[1741] CEDH, 18 janvier 1978, *Irlande c. Royaume-Uni*, n° 5310/71, §207 [en ligne].

[1742] Voir notamment : SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, spéc. pp. 39-42 ; KISSANGOULA (J.), « La sécurité dans la jurisprudence de la CEDH », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 229-252, spéc. pp. 251-252 ; ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, spéc. p. 280.

[1743] SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, p. 39.

[1744] *Ibid*.

[1745] CEDH, 1er juillet 1961, *Lawless c. Irlande*, *op. cit.*, n° 3, § 22 : L'État partie dispose du droit d'appliquer l'article 15 « sous la condition que ces mesures soient strictement limitées aux exigences de la situation et qu'en outre elles ne soient pas en contradiction avec les autres obligations découlant du droit international ; qu'il appartient à la Cour de vérifier si les conditions énumérées à l'article 15 (art. 15) pour l'exercice du droit exceptionnel de dérogation [sont] réunies ». Pour exemple, les autorités françaises ont eu recours à la dérogation prévue par l'article 15 de la Conv.EDH pour déclarer l'état d'urgence lors des violences urbaines de 2005 ainsi que lors des attentats terroristes à Paris en novembre 2015 (SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, p. 27). En revanche, elles n'avaient pas souhaité recourir à ce régime dérogatoire lors de la pandémie de COVID-19 en 2020. Les avis divergent au sein de la doctrine quant au choix adopté. S'il est incontestable que les mesures mises en œuvre remplissaient les conditions de l'article 15 de la Conv.EDH, certains auteurs perçoivent positivement l'application de mesures restrictives plutôt que dérogatoires ; les premières étant plus strictement encadrées par la CEDH (TOUZÉ (S.), « La restriction vaudra toujours mieux que la dérogation… », *JCP G* n° 17, 27 avril 2020, act. 511). En revanche d'autres auteurs soutiennent que le contrôle de ces mesures par la CEDH ne serait que de pur forme (SUDRE (F.), « La mise en quarantaine de la Convention européenne des droits de l'homme », *JCP G* n° 17, 27 avril 2020, act. 510).

d'appréciation » accordée aux États en faisant jouer le principe de subsidiarité[1746]. Ces dernières années, la CEDH fonde davantage son approche sur « la reconnaissance d'obligations positives procédurales aux États » adoptant des mesures restrictives des droits et libertés issues de la Conv.EDH que sur « l'affirmation forte d'une obligation de limiter »[1747] ces mesures. Il en va notamment ainsi concernant le recours à des technologies de surveillance de masse par les États dont le traitement des données collectées, essentiellement à caractère personnel, vise à remplir un objectif de sécurité nationale.

2. L'assouplissement du contrôle des mesures restrictives des droits et libertés dans la jurisprudence de la Cour européenne des droits de l'homme

616. La révolution technologique a conduit la CEDH à fonder ses décisions sur des droits qui ne sont pas mentionnés dans la Conv.EDH[1748] puisque, de fait, celle-ci n'a pas fait l'objet d'une révision afin d'y intégrer les sujets liés au numérique[1749]. Il en va ainsi plus particulièrement du droit de la protection des données à caractère personnel[1750] qui est uniquement rattaché à l'article 8 de la Conv.EDH relative à la protection de la vie privée et des correspondances[1751]. À titre d'exemple, le juge européen des droits de l'homme reconnait une protection des DACP collectées au sein de l'espace public sur le fondement de l'article 8 de la Conv.EDH[1752]. Afin de prendre en compte les enjeux liés au numérique, la jurisprudence de la CEDH repose sur une interprétation de la Conv.EDH adaptée au contexte actuel ainsi que sur la Convention 108 du Conseil de l'Europe

---

[1746] SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, p. 42 ; ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, p. 283 ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.* ; DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.*

[1747] DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.*

[1748] ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, pp. 271-272.

[1749] À l'inverse de l'Union européenne qui, à titre d'exemple, a inséré à l'article 8 de la CDFUE des dispositions en matière de protection des DACP.

[1750] Le droit à la protection des DACP a de fait été reconnu comme jouant « un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention » (CEDH, gr. ch., 26 juin 2017, *Satakunnan markkinapörsii Oy et Satamedia Oy c. Finlande*, n° 931/13, §137 [en ligne]).

[1751] CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04, n° 30566/04, §67 [en ligne].

[1752] Voir en ce sens : CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, *op. cit.*, §59 où l'affaire portait sur l'enregistrement et la diffusion d'images issues d'une vidéosurveillance installée dans un lieu public.

portant sur la protection des données à caractère personnel[1753] et aussi, parfois, sur la jurisprudence de la CJUE[1754].

617. Pour l'heure, la CEDH n'a pas encore eu l'occasion de juger une affaire directement liée à des technologies reposant sur de l'IA[1755], telle que les drones aériens « augmentés » de sécurité publique. Néanmoins, plusieurs décisions en lien avec les nouvelles technologies, dont les algorithmes, ont été rendues par le juge européen des droits de l'homme. Ces décisions portaient essentiellement sur des violations du droit au respect de la vie privée et de la correspondance[1756] et du droit à la liberté d'expression[1757] mais aussi, plus rarement, du principe de non-discrimination[1758] notamment s'agissant d'affaires relatives à la surveillance de masse[1759], sans analyser l'incidence d'un traitement de DACP par les algorithmes d'IA[1760]. Ainsi, la CEDH a eu l'occasion de rendre des décisions dans le cadre d'affaires portant sur le recours à des mesures de prévention des infractions et sur le recours à des technologies à des fins de surveillance de masse par les États[1761].

618. Le contrôle variable des mesures de prévention des infractions - La CEDH a rendu une décision le 29 juin 2006 sur l'affaire *Weber et Saravia c. Allemagne*[1762] où les requérants

---

[1753] La Convention n° 108 du Conseil de l'Europe devrait prochainement faire l'objet d'un amendement sous l'appellation de Convention 108 + dont l'objectif est de répondre aux enjeux liés au numérique et intégrer les questions relatives aux algorithmes ainsi qu'à l'IA [en ligne].

[1754] Voir à titre principal : CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.* ; CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*

[1755] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 20 ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 316.

[1756] Conv.EDH, art. 8, §1 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ».

[1757] Conv.EDH, art. 10, §1 : « Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière ».

[1758] Conv.EDH, art. 14 : « La jouissance des droits et libertés reconnus [par la] Convention doit être assurée, sans distinction aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation ».

[1759] CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.* ; CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.* ; CEDH, gr. ch., 4 décembre 2015, *Roman Zakharov c. Russie*, *op. cit.*

[1760] CEDH, Fiche thématique « Nouvelles technologies » [en ligne].

[1761] Bien que les affaires portant sur la surveillance de masse soit relatif à la sécurité nationale, et non à la sécurité publique, l'analyse des arrêts *Centrum för Rättvisa c. Suède* et *Big Brother Watch et autres c. Royaume-Uni* présente un certain intérêt compte tenu du fait qu'ils traitent du sujet de la lutte contre les menaces terroristes, une des finalités prévues en matière de recours à des drones aériens de sécurité publique (CSI, art. L; 242-5 3°).

[1762] CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, n° 54934/00 [en ligne].

contestaient plusieurs dispositions de la loi allemande du 13 août 1968 relative aux restrictions du secret de la correspondance, des envois postaux et des télécommunications modifiée par une loi du 28 octobre 1994. L'affaire portait essentiellement sur l'amplification des pouvoirs de renseignement de l'État fédéral allemand lui permettant d'avoir recours à des algorithmes d'enregistrement des télécommunications et d'utiliser les DACP extraites à des fins de prévention des infractions dans le cadre d'une surveillance dite « stratégique »[1763]. Sur l'abus éventuel des pouvoirs de surveillance de l'État, le juge européen des droits de l'homme avait estimé que les dispositions contestées comprenaient suffisamment de « garanties adéquates et effectives contre les abus éventuels des pouvoirs de surveillance stratégique de l'État » et qu'en tout état de cause l'État fédéral allemand disposait d'une « marge d'appréciation relativement large en la matière »[1764].

619. Le juge européen des droits de l'homme a par la suite confirmé sa position offrant une certaine latitude aux États en matière de sécurité nationale prenant en considération la menace permanente du terrorisme international[1765]. La CEDH a néanmoins dérogé à sa position dans le cadre de sa décision du 1er juillet 2008 concernant l'affaire *Liberty et autres c. Royaume-Uni*[1766] où elle a sanctionné la loi qui avait été adoptée portant sur l'interception de communications considérant qu'elle portait atteinte au droit à la vie privée protégé par l'article 8 de la Conv.EDH. Dans cette affaire, elle a estimé que la loi ne présentait pas de garanties suffisantes contre les abus de pouvoirs de l'État et que le contenu du pouvoir d'appréciation des autorités publiques n'était pas clairement défini[1767].

620. Une protection décevante contre la surveillance de masse - Le juge européen des droits de l'homme n'a pu que constater la propension des États à recourir à des moyens technologiques intrusifs en vue de renforcer la sécurité des personnes et des biens dans les combats menés face à la menace du terrorisme et de la criminalité transfrontalière[1768]. Face aux traitements massifs de données effectués par les États, la CEDH a décidé de transposer sa jurisprudence en

---

[1763] *Idem*, §4.

[1764] *Idem*, §137.

[1765] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 321.

[1766] CEDH, gr. ch., 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, n° 58243/00 [en ligne].

[1767] *Idem*, §§66, 67 et 69.

[1768] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, 15, p. 115.

matière d'interception des communications à des fins de sécurité nationale[1769] tout en l'accordant aux particularités liées aux nouvelles technologies[1770]. Suite aux révélations d'Edward Snowden, ancien agent de l'Agence nationale de sécurité américaine (NSA), en 2013[1771], la CEDH a été saisie de deux affaires significatives portant sur la surveillance de masse, *Centrum för Rättvisa c. Suède* et *Big Brother Watch et autres c. Royaume-Uni*, dont les décisions finales ont été rendues le 25 mai 2021. Si elle a condamné les deux États défendeurs au motif qu'ils contrevenaient au droit au respect de la vie privée au moyen de mesures exceptionnelles mises en œuvre à des fins d'interception massive de données, elle a néanmoins rejeté l'argument portant sur la violation de la Conv.EDH par un transfert de ces données à des services de renseignement étrangers[1772].

621. Dans l'arrêt *Centrum för Rättvisa c. Suède*, les requérants avaient contesté la législation autorisant l'interception massive de signaux électroniques à des fins de renseignement étranger au motif qu'elle portait atteinte à l'article 8 de la Conv.EDH relatif au droit à la vie privée. Dans ses premières observations, la CEDH a estimé que « l'article 8 de la convention n'interdit pas l'interception en masse afin de protéger la sécurité nationale ou d'autres intérêts nationaux essentiels contre des menaces extérieures graves » et que « les États jouissent d'une ample marge d'appréciation pour déterminer de quel type de régime d'interception ils ont besoin à cet effet »[1773]. Cette affirmation reprend ainsi les conclusions issues des arrêts *Weber et Saravia c. Allemagne* et *Liberty et autres c. Royaume-Uni*[1774]. Néanmoins, elle a rappelé que la marge d'appréciation laissée aux États parties à la Conv.EDH est soumise à un contrôle de proportionnalité permettant de palier les risques d'arbitraire et d'abus et que les mesures restrictives doivent présenter des garanties suffisantes[1775]. La CEDH a considéré que la loi contestée méritait certaines améliorations mais que le « système suédois d'interception en masse a révélé que celui-ci est fondé sur des règles juridiques

---

[1769] CEDH, gr. ch., 6 septembre 1978, *aff. Klass et autres c. Allemagne*, *op. cit.*, §§48 et 49.

[1770] ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, p. 283.

[1771] Le lanceur d'alerte avait révélé l'existence de traitements massifs de DACP par un des services de renseignement britannique (*Government Communications Headquarters*) et par la NSA auprès des fournisseurs d'accès à Internet. Voir pour exemple : "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, June 11th 2013 [en ligne].

[1772] CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, §§395 et 398.

[1773] CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.*, §261.

[1774] CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, *op. cit.*, §§78 et 79 ; CEDH, gr. ch., 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, *op. cit.*, §57.

[1775] CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.*, §261.

détaillées, que sa portée est clairement délimitée et qu'il offre des garanties […] adéquates contre les abus »[1776]. Constatant ensuite trois carences du système suédois d'interception en masse[1777] (l'absence de règles claires concernant la destruction des données interceptées, l'exclusion des éléments relatifs à la vie privée dans les lois en matière de renseignement, l'absence de contrôle *a posteriori*), la Chambre a reconnu l'atteinte au droit au respect de la vie privée[1778] et condamné l'État suédois.

622. De manière similaire, l'affaire *Big Brother Watch et autres c. Royaume-Uni* avait été initiée par une organisation non-gouvernementale qui alléguait une atteinte aux articles 8 et 10 de la Conv.EDH par un programme de surveillance et de partage de renseignements entre les États-Unis et le Royaume-Uni permettant l'interception massive de communications[1779]. Là encore, la CEDH a avancé la marge d'appréciation des États[1780] et l'intérêt légitime de ces derniers à mettre en œuvre des systèmes de surveillance de masse[1781]. À l'issue de son analyse, elle a condamné l'État britannique en raison de trois manquements majeurs concernant l'absence d'autorisation indépendante des interceptions, le manque de précision concernant les données traitées ainsi que l'absence de filtrage individuel, considérant ainsi que la loi ne présentait pas les garanties suffisantes et adéquates contre les risques d'abus et d'arbitraire[1782]. Toutefois, il est surprenant que les juges n'aient pas admis la violation de l'article 8 de la Conv.EDH concernant le transfert des données collectées sur le territoire de l'État britannique (État membre) vers les États-Unis[1783] alors que la CJUE avait conclu à l'application du droit à la protection des données dans des affaires

---

[1776] *Idem*, §367.

[1777] *Idem*, §369.

[1778] *Idem*, §374.

[1779] CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, §266.

[1780] *Idem*, §274.

[1781] *Idem*, §323.

[1782] *Idem*, §425 : La loi contestée « ne renfermait pas suffisamment de garanties "de bout en bout" pour offrir une protection adéquate et effective contre l'arbitraire et le risque d'abus ». La CEDH « relève notamment que ce régime présentait des lacunes fondamentales, à savoir l'absence d'autorisation indépendante, l'absence de mention des catégories de sélecteurs dans les demandes de mandat et le fait que les sélecteurs liés à un individu n'étaient pas soumis à une autorisation interne préalable ».

[1783] *Idem*, §§395 et 398. Voir sur le sujet : DANIS-FATÔME (A.), « Sécurité nationale et protection des données : quelle articulation ? », *Communication et commerce électronique* n° 9, septembre 2021, comm. 66.

similaires[1784]. Enfin, la CEDH a rejeté le motif d'atteinte à la liberté de communication des journalistes (sur la base de l'article 10 de la Conv.EDH)[1785].

623. Dans les deux affaires, la CEDH a adopté une position favorable aux États estimant qu'ils ont un intérêt légitime à recourir à la surveillance de masse[1786] et a constaté « l'importance vitale » que présente l'interception en masse des données à des fins de détection des menaces pesant sur la sécurité nationale[1787]. Elle a rendu des décisions « en demi-teinte » dans la mesure où elle a défini les conditions nécessaires pour qu'un régime de surveillance de masse puisse être compatible avec les articles 8 et 10 de la Conv.EDH[1788]. Ainsi, elle a manqué l'opportunité de marquer l'importance du droit au respect de la vie privée en gardant une approche favorisant davantage la protection des droits du collectif au détriment des droits individuels[1789]. En matière de sécurité, publique comme nationale, la CJUE se montre nettement moins conciliante avec les États.

B. Les technologies de surveillance sous le regard du juge de l'Union européenne

624. À l'origine, la CJUE, autrefois appelée Cour de justice des Communautés européennes (CJCE), ne disposait pas de procédure spécifique pour faire respecter les droits et libertés en raison notamment d'une absence dans les premiers traités des dispositions portant sur le sujet[1790]. Prenant exemple sur les juridictions de plusieurs États membres, le juge de l'Union européenne a commencé

1784 CJUE, gr. ch., 6 octobre 2015, *Schrems I*, aff. C-362/14 [en ligne] ; CJUE, gr. ch., 16 juillet 2020, *Schrems II*, aff. C-311/18 [en ligne].

1785 CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, §430 : « les mesures de surveillance relevant du régime institué […] ne visaient pas à surveiller les journalistes ni à découvrir leurs sources, l'interception de ces communications ne pouvaient [...] être qualifiée d'atteinte particulièrement grave à la liberté d'expression ».

1786 CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.*, §§ 236 et 237 ; CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, §§322 et 323.

1787 CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.*, §365 ; CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, §424.

1788 DANIS-FATÔME (A.), « Sécurité nationale et protection des données : quelle articulation ? », *op. cit.* ; DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.*

1789 DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.* : « la CEDH manque une occasion de mettre en avant le caractère particulièrement sensible du droit au respect de la vie privée […] qui lui aurait permis de justifier une restriction de cette marge d'appréciation compte tenu de la gravité de l'intrusion de ce type de mesure dans la vie privée des individus » ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.* : « La Cour s'éloigne ainsi progressivement de son rôle initial de protection des droits individuels ».

1790 DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, pp. 96-97.

par consacrer plusieurs principes généraux du droit[1791]. Il a ainsi reconnu pour la première fois le droit au respect de la vie privée dans un arrêt *National Panasonic c. Commission* le 26 juin 1980 par l'intermédiaire de l'article 8 de la Conv.EDH[1792]. La jurisprudence de la CJUE en matière de protection des droits et libertés a servi à inspirer la rédaction[1793] et la révision des textes européens[1794]. Cependant, le droit de l'Union européenne inclut comme particularité le fait que les droits et libertés qu'il proclame « ne lient les États-membres que pour autant qu'est en cause une situation régie par le droit de l'Union européenne »[1795]. Aujourd'hui, la CJUE assure la protection de nombreux droits et libertés et est même devenue un acteur majeur du domaine[1796]. En matière d'usages technologiques, elle s'appuie essentiellement sur le droit étendu de la protection des DACP ainsi que sur son contrôle de l'ingérence dans un droit qu'elle reconnait comme fondamental (1). Elle a ainsi eu l'occasion de rendre plusieurs décisions portant sur la collecte et la conservation massive de DACP, notamment à des fins de sécurité publique ou de sécurité nationale (2).

1. Les mécanismes de protection des droits et libertés du juge de l'Union européenne

625. L'affirmation du droit à la protection des données à caractère personnel - La jurisprudence de la CJUE joue un rôle essentiel dans l'encadrement des technologies portant sur la collecte de données et peut rendre des décisions concernant des technologies reposant sur des technologies d'IA bien qu'elle n'ait encore que rarement eu l'occasion d'examiner les effets de leurs usages[1797]. À cette fin, le juge de l'Union européenne recourt principalement au droit à la vie privée et au droit à la protection des données à caractère personnel pour rendre ses décisions en la matière[1798]. Ainsi, la CJUE tire ses fondements de la CDFUE qui comprend des dispositions

---

[1791] À titre d'exemple : CJCE, 21 juin 1958, *Hauts fourneaux et aciéries belges*, aff. 8/57 [en ligne] ; CJCE, 17 décembre 1970, *Internationale Handelgesellschaft*, aff. 11/70 [en ligne].

[1792] CJCE, 26 juin 1980, *National Panasonic c. Commission*, aff. 136/79, §17 [en ligne].

[1793] La jurisprudence de la CEDH ainsi que celle de la CJUE ont initié la rédaction de la CDFUE adoptée le 7 décembre 2000 et entrée en vigueur le 1er décembre 2009.

[1794] Le Traité sur le fonctionnement de l'Union européenne (TFUE), dans sa rédaction suite au Traité de Maastricht du 7 février 1992, avait validé les décisions juridictionnelles de la CJUE en considérant que « les droits fondamentaux font partie du droit de l'Union en tant que principes généraux du droit » (art. 6).

[1795] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 98.

[1796] LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, *op. cit.*, p. 118.

[1797] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance, 31 mars 2022, *op. cit.*, (Annexe 10) p. 358.

[1798] *Idem*.

relatives au respect du droit à la vie privée[1799] ainsi que du droit à la protection des données à caractère personnel[1800]. En outre, elle admet une conception étendue de la notion de données à caractère personnel[1801], considérant qu'elle comprend « toute information concernant une personne physique identifiée ou identifiable »[1802] incluant « tout élément qui particularise la personne et qui est de nature à permettre son identification »[1803]. Les données peuvent dès lors être qualifiées de données à caractère personnel même lorsqu'elles ne contiennent pas d'informations dont la communication est susceptible de causer un préjudice à la personne concernée[1804]. Ce droit consacré des DACP lui a ainsi permis « d'être au cœur de certaines des problématiques contemporaines les plus épineuses »[1805]. Il constitue une garantie effective dans la mesure où il est opposable tant aux acteurs privés qu'aux acteurs publics et qu'il s'est imposé au sein de la jurisprudence de la CJUE.

626. La méthode de contrôle de l'ingérence dans les droits fondamentaux de l'Union européenne - La CJUE contrôle l'ingérence dans l'exercice des droits fondamentaux sur le fondement de l'article 52 §1 de la Charte des droits fondamentaux de l'Union européenne[1806]. À l'appui de cette disposition, il est possible de dégager trois principes au contrôle exercé par le juge de l'Union européenne. En premier lieu, la CJUE doit s'assurer que le principe de limitation de l'exercice des droits fondamentaux de l'UE est « prévu par la loi ». S'appuyant sur la jurisprudence de la CEDH[1807], le juge de l'Union européenne a précisé que « les restrictions [aux droits fondamentaux] doivent être prévues par des dispositions normatives libellées de façon suffisamment précise pour permettre aux intéressés de régler leur conduite en s'entourant au besoin

---

[1799] CDFUE, art. 7.

[1800] CDFUE, art. 8, §1 : « toute personne a le doit à la protection des données à caractère personnel la concernant ».

[1801] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 235.

[1802] CJUE, gr. ch., 9 novembre 2010, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09, §52 [en ligne].

[1803] Voir par exemple : CJCE, 29 janvier 2008, *Promusicae c. Telefonica de Espana*, aff. C-275/06 sur la reconnaissance de l'adresse IP comme étant une donnée à caractère personnel indirectement identifiante.

[1804] CJCE, 20 mai 2003, *Österreichischer Rundfunk*, aff. jointes C-465/00, C-138/00, C-139/01, §75 [en ligne].

[1805] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 237.

[1806] CDFUE, art. 52 §1 : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

[1807] CEDH, 26 avril 1979, *Sunday Times c. Royaume-Uni*, n° 6538/74, §49 [en ligne].

de conseils éclairés »[1808]. En deuxième lieu, il s'assure que les mesures restrictives des droits et libertés sont « nécessaires » et poursuivent un « objectif d'intérêt général » ou « la protection des droits et libertés d'autrui ». Cette condition inclut notamment la sauvegarde de l'ordre public[1809]. En dernier lieu, le juge de l'Union européenne effectue un contrôle de proportionnalité de l'objectif d'intérêt général afin de déterminer s'il peut « justifier des conséquences négatives » sur les personnes concernées[1810] (v. **n° 828 et suiv.**).

2. Le contrôle strict des mesures de conservation des données à caractère personnel à des fins de surveillance

627. L'interdiction de la conservation généralisée et indifférenciée des données à des fins de sécurité - La CJUE a développé une large jurisprudence en matière de contrôle des mesures portant sur la surveillance de masse des données, y compris à caractère personnel, à des fins de sécurité nationale ou de sécurité publique[1811]. Elle s'est illustrée, en premier lieu, lors d'une décision d'assemblée dans le cadre de l'affaire *Digital Rights Ireland Ltd. e. a.* du 8 avril 2014[1812]. L'arrêt avait conduit à l'invalidation de la directive 2006/24/CE du 15 mars 2006[1813], portant sur la conservation des données par les fournisseurs de services de communications électroniques, dont les dispositions contraignaient ces derniers à conserver l'ensemble des métadonnées de leurs utilisateurs permettant leur exploitation ultérieure par les forces de l'ordre à des fins d'enquête. La CJUE avait considéré, en premier lieu, que la conservation des métadonnées entrait dans le cadre des articles 7 et 8 de la CDFUE dans la mesure où leur utilisation est susceptible de permettre de « tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été

[1808] CJCE, 6 mars 2001, *Connolly c. Commission*, aff. C-274/99P, § 42 [en ligne].

[1809] Voir notamment : CJCE, 28 octobre 1975, *Rutili c. ministre de l'intérieur*, aff. 36-75, § 47 [en ligne].

[1810] Voir notamment : CJCE, gr. ch., 3 septembre 2008, *Kadi c. Conseil de l'Union européenne et Commission des communautés européennes*, aff. jointes C-402/05 P et C-415/05 P, § 363 [en ligne] (lutte contre les actes de terrorisme).

[1811] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 496.

[1812] CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, aff. jointes C-293/12 et C-594/12, §73 [en ligne].

[1813] Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *JOUE* L 105 du 13 avril 2006, p. 54 [en ligne].

conservées »[1814]. Elle avait ajouté, en deuxième lieu, que les dispositions de la directive en cause constituaient une « ingérence […] particulièrement grave »[1815] à l'exercice de ces droits.

628. Une protection stricte contre la surveillance de masse - Reprise dans un arrêt de principe, les conclusions de l'affaire *Digital Rights Ireland Ltd. e. a.* ont inspiré la CJUE dans plusieurs autres affaires énonçant l'incompatibilité avec le droit de l'Union européenne de toute conservation généralisée et indifférenciée des métadonnées des utilisateurs de communications électroniques, y compris à des fins de sécurité nationale[1816]. Néanmoins, elle admet que des données puissent être conservées à des fins de lutte contre la criminalité ou les atteintes à la sécurité nationale[1817] sous réserve que le traitement soit limité à ce qui est strictement nécessaire à la poursuite de ces finalités[1818]. Dès lors, la CJUE serait compétente pour déterminer si le traitement de DACP au moyen de drones aériens de sécurité publique, faisant éventuellement l'objet d'une analyse par un algorithme d'aide à la prise de décisions, est proportionné au regard des besoins en matière de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions.

629. Dans sa décision *La Quadrature du Net et a.* du 6 octobre 2020[1819], la CJUE s'était encore démarquée comme étant l'une des protectrices des individus quant au recours à des technologies de surveillance de masse[1820]. À cette occasion, elle a confirmé le principe d'interdiction de la surveillance de masse dégagé lors de ses décisions précédentes[1821]. La CJUE a néanmoins assoupli sa position en admettant la possibilité pour les États d'y recourir en raison de

---

[1814] CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, *op. cit.*, §27.

[1815] *Idem*, § 37.

[1816] CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, aff. jointes C-203/15 et C-698/15 [en ligne] ; CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, aff. jointes C-511/18, C-512/18 et C-520/18, *op. cit.* ; CJUE, gr. ch., 6 octobre 2020, *Privacy International*, aff. C-623/17 [en ligne] ; CJUE, gr. ch., 28 septembre 2023, *La Quadrature du Net e. a. II*, aff. C-470/21 [en ligne].

[1817] À titre d'exemple, la CJUE avait validé la conservation généralisée de données s'agissant du système *Passager Name Record* (CJUE, gr. ch., 26 juillet 2017, *Avis rendu en vertu de l'article 218, paragraphe 11, avis 1/15*, §§ 190-211 [en ligne]). Voir aussi : CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, *op. cit.*, spéc. §115.

[1818] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 236.

[1819] CJUE, 6 octobre 2020, *La Quadrature du Net et a.*, aff. jointes C-511/18, C-512/18 et C-520/18, *op. cit.*

[1820] DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *op. cit.*

[1821] CJUE, 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.*, §111. Voir : CJUE, 21 décembre 2016, *Tele2 Sverige*, *op. cit.*, §§ 89 et 104.

motifs de sécurité nationale[1822], qu'elle définit de manière stricte[1823]. Dès lors, elle n'admet cette exception au principe d'interdiction de la surveillance de masse uniquement en raison de l'objectif de préservation de la sécurité nationale (condition spécifique) qui dépasse les objectifs de sécurité publique et de lutte contre la criminalité[1824]. Si la CJUE déroge à son principe, elle exerce néanmoins un contrôle strict des dispositions des États membres en matière de traitement massif de données à caractère personnel.

630. Conclusion - Bien que la CEDH soit parfois perçue comme l'initiatrice de la protection des données à caractère personnel dans la jurisprudence européenne[1825], c'est pourtant la CJUE qui assure le contrôle le plus rigoureux en la matière, notamment s'agissant des données collectées dans le cadre de la sécurité nationale à des fins de lutte contre le terrorisme[1826]. En ce sens, la Cour de justice soumet le traitement des DACP à des conditions plus strictes[1827]. Dès lors, le juge européen des droits de l'homme pourrait se montrer clément à l'égard des autorités publiques qui auraient recours à des drones aériens « augmentés » de manière disproportionnée notamment à des fins de lutte contre le terrorisme. De fait, la CEDH pourrait de nouveau alléguer que l'État mis en cause dispose d'un intérêt légitime, compte tenu des nombreuses menaces qui pèsent sur la sécurité publique, permettant de rejeter le caractère disproportionné de ces usages et faire valoir la marge d'appréciation des États en matière de surveillance de masse[1828]. Au regard de la jurisprudence européenne, la CJUE présente davantage d'opportunités de renforcer les garanties des droits et

---

[1822] CJUE, 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.*, §110.

[1823] *Idem*, §135 : La sécurité nationale « correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme ».

[1824] *Idem*, §§140-141.

[1825] SUDRE (F.), *Droit européen et international des droits de l'homme*, *op. cit.*, p. 721 : « fondant son contrôle sur la CDFUE (article 7 et 8), la CJUE reprend à son compte l'interprétation de l'article 8 de la CEDH par la Cour de Strasbourg relative à la vie privée et à la protection des données à caractère personnel ».

[1826] ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, spéc. pp. 282-283.

[1827] Voir notamment en ce sens : CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd et a.*, *op. cit.* ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, *op. cit.* ; CJUE, 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.* ; CJUE, gr. ch., 28 septembre 2023, *La Quadrature du Net e. a. II*, *op. cit.*

[1828] Voir en ce sens : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 323 : « Pour la Cour, le principe de ce système de surveillance de masse [système d'interception des communications] n'appelle pas de critique et confirme la large marge d'appréciation laissée en la matière aux États membres, ce qui permettrait potentiellement d'y inclure des systèmes basés sur des « IA » ». L'auteur ajoute que « les révélations d'Edward Snowden, dévoilant le système de surveillance de masse organisé par les services de renseignement américains, la banalisation de tels systèmes, en Europe et ailleurs, s'appuie de manière opportune sur la crainte terroriste ».

libertés quant aux usages des technologies de surveillance de sécurité publique. Elle n'est pas la seule à garantir les droits et libertés face à la multiplication des technologies de surveillance. Les institutions non-juridictionnelles, à commencer par la CNIL, prétendent également au rang de protecteur essentiel au maintien effectif de l'exercice des droits et libertés dans ce contexte qui laisse une place conséquente au numérique.

§2. Les autorités administratives indépendantes, rempart des droits et libertés

631. L'engouement pour l'emploi de technologies de surveillance par les forces de l'ordre n'a pas non plus échappé aux différentes autorités non-juridictionnelles chargées de défendre les droits et libertés. Parmi elles, la CNIL joue un rôle prépondérant concernant tous les sujets ayant trait aux nouvelles technologies, dont celles à l'usage des autorités publiques, et ne manque pas de faire usage de ses pouvoirs de recommandation et de sanction pour faire garantir au mieux les droits et libertés des personnes concernées par un traitement de DACP[1829] (A). Dans un rôle non moins essentiel, le Défenseur des droits dispose aussi de différents pouvoirs pour assurer le maintien des droits et libertés face aux usages de moyens technologiques des autorités publiques, principalement à des fins de surveillance (B).

A. Le rôle pilier de la CNIL dans la protection des droits et libertés

632. Pour faire face aux nombreuses missions qui lui ont été attribuées, la CNIL exerce différents pouvoirs qui ont été progressivement renforcés en vue d'assurer le respect des droits et libertés notamment quant à l'usage de technologies de surveillance par les forces de l'ordre (1). Néanmoins, si la CNIL exerce son rôle avec diligence, elle pâtit toujours d'un manque de moyens dont les répercussions pourraient être aggravées par l'arrivée imminente d'une forme « augmentée » de ces technologies par des algorithmes d'aide à la prise de décisions (2).

[1829] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 230.

1. Le pouvoir de contrôle de la CNIL sur les technologies de surveillance de sécurité publique

633. Dès les années 1970, le développement exponentiel de l'informatique inquiète quant à sa puissance de traitement et de stockage des données (de toute nature) ainsi qu'aux possibilités d'interconnexions des informations pouvant porter une atteinte grave aux droits et aux libertés[1830]. Ces craintes n'ont eu de cesse de s'accroitre face aux progrès toujours plus rapides des développements technologiques. Très tôt, le législateur français a pris la mesure des enjeux entourant le traitement des données et l'incidence qu'il présente pour les droits et libertés. Au travers de la LIL du 6 janvier 1978, le législateur a offert pour la première fois un encadrement à l'usage de l'informatique en formulant les grands principes à respecter et en introduisant une nouvelle autorité de contrôle, la CNIL[1831].

634. La CNIL, en tant qu'autorité administrative indépendante, est chargée de veiller au respect de la protection de la vie privée et des DACP. Depuis sa création, la CNIL n'a eu de cesse d'évoluer afin de faire face aux développements exponentiels de nouvelles technologies. Celles-ci se sont multipliées et complexifiées, notamment dans le domaine de la surveillance de la voie publique[1832], mettant toujours plus en difficultés la CNIL dans son rôle de contrôle de leurs usages et de la protection des droits et libertés[1833]. Afin de pallier ces évolutions technologiques et la multiplication de leurs usages, le législateur a renforcé les pouvoirs de contrôle de la CNIL. Elle a pour mission de veiller à la conformité des traitements mis en œuvre à la règlementation relative à la protection des DACP[1834] et donne notamment des avis concernant les traitements de DACP effectués pour le compte de l'État à des fins de sécurité publique[1835]. Elle est compétente pour

---

[1830] HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 484 : À ce sujet, le projet intitulé SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) avait fait polémique en raison de ses finalités « d'interconnexion de l'ensemble des fichiers nominatifs de l'administration française par le biais du numéro INSEE ».

[1831] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 75.

[1832] Voir notamment : CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », 19 juillet 2022, *op. cit.*

[1833] Voir notamment : CNIL, Rapport de synthèse du débat public animé par la CNIL sur les enjeux éthiques des algorithmes et de l'intelligence artificielle « Comment permettre à l'Homme de garder la main ? - Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle », décembre 2017, *op. cit.* ; CNIL, Rapport annuel de 2022 « Agir pour un futur numérique responsable », *cnil.fr*, mai 2023 [en ligne].

[1834] LIL, art. 8, I.

[1835] LIL, art. 31.

publier des lignes directrices, recommandations ou référentiels afin de faciliter la mise en conformité des traitements de DACP avec les textes[1836].

635. Parmi ses missions, la CNIL collabore avec d'autres institutions publiques à la recherche de solutions permettant d'assurer une meilleure protection des droits et libertés[1837]. Aussi, elle peut formuler des observations devant toutes les juridictions[1838] s'agissant des litiges relatifs à la protection des DACP[1839]. Le Conseil d'État a reconnu que, dans le cadre de son pouvoir de dénonciation au Parquet des infractions dont elle a connaissance, la CNIL disposait d'une appréciation discrétionnaire soumise à un contrôle restreint de l'établissement des faits et de l'existence d'une atteinte caractérisée portant sur les dispositions dont elle assure le respect[1840]. Enfin, la CNIL dispose d'un pouvoir de sanction (rappel à l'ordre, injonction, retrait de certification, etc.)[1841]. Elle a notamment eu l'occasion de procéder à des sanctions du ministère de l'Intérieur concernant des fichiers de police[1842].

636. En matière de vidéoprotection, le législateur a confié à la CNIL le soin d'émettre un avis précédent la publication du décret autorisant la mise en œuvre d'un système de vidéoprotection[1843] et de réceptionner les analyses d'impact à la protection des DACP. À défaut, la CNIL est compétente pour sanctionner les autorités publiques. Le recours à des drones aériens équipés de caméras par la Préfecture de police de Paris lors des confinements en 2020 avait ainsi donné lieu à une sanction de la CNIL[1844] au motif que le ministère de l'Intérieur avait manqué à l'obligation de

---

1836 LIL, art. 8, I, 2), b).

1837 À titre d'exemple : DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020, *op. cit.* (rapport co-écrit avec le Défenseur des droits).

1838 HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 490.

1839 LIL, art. 8, I, 5).

1840 CE, sect., 27 octobre 1999, n° 196306 [en ligne] : « il appartient à la commission nationale de l'informatique et des libertés d'aviser le procureur de la République des faits dont elle a connaissance dans l'exercice de ses attributions, si ces faits lui paraissent suffisamment établis et si elle estime qu'ils portent une atteinte suffisamment caractérisée aux dispositions dont elle a pour mission d'assurer l'application ».

1841 LIL, art. 16.

1842 CNIL, « Fichier automatisé des empreintes digitales : rappel à l'ordre du ministère de l'Intérieur », *cnil.fr*, 30 septembre 2021 [en ligne].

1843 CSI, art. L. 255-1 (caméras fixes) et L. 242-8 (drones aériens) : L'utilisation des DACP collectées par les systèmes de vidéoprotection (fixes et mobiles) sont précisées par un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés.

1844 CNIL, Délibération n°SAN-2021-003, *op. cit.*

lui remettre une analyse d'impact sur la protection des DACP en application des dispositions de la LIL et de la DPJ[1845].

637. La CNIL peut également formuler des avis concernant des projets de lois ou des décrets portant sur la protection des DACP afin de soumettre des propositions d'adaptation des dispositions[1846]. Il convient cependant de noter que ses avis ne font office ni d'une « autorisation » ni d'un « refus » et entendent uniquement porter à l'attention des pouvoirs publics les enjeux en matière d'informatique, de fichiers et de libertés. La CNIL avait ainsi émis un avis le 26 janvier 2021 concernant le projet de loi « sécurité globale » soulignant une amplification des enjeux concernant à titre principal le recours à des drones aériens en vue de filmer l'espace public[1847]. En décembre 2022, elle avait également publié un avis portant sur le projet de loi JOP2024 concernant l'autorisation d'une expérimentation de caméras « augmentées » filmant l'espace public[1848]. À cette occasion, la CNIL avait déclaré que le recours à ces technologies constituait « une modification de la nature des dispositifs vidéo »[1849]. Son avis s'était révélé globalement favorable au texte qui apportait selon elle un certain nombre de garanties permettant de limiter les atteintes aux DACP. Néanmoins, elle soulignait qu'en aucun cas cette expérimentation ne « préjugeait d'une éventuelle pérennisation de ces systèmes »[1850]. Aussi, elle avait jugé nécessaire que « les critères permettant de déterminer leur périmètre de déploiement soient appréciés de manière restrictive » et que les évènements prédéterminés « devraient être sélectionnés au regard des performances des traitements algorithmiques » afin d'assurer leur fiabilité[1851]. Enfin, s'agissant du droit à l'information des personnes concernées, la CNIL avait insisté sur la nécessité de limiter les hypothèses excluant la

---

[1845] Obligation des autorités publiques de remettre une analyse d'impact sur la protection des DACP en vertu des articles 90 de la LIL et 27 de la DPJ remplaçant la procédure d'autorisation de procéder à un traitement de DACP par l'intermédiaire d'un dispositif de vidéoprotection.

[1846] LIL, art. 8, I, 4), a).

[1847] CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, *op. cit.*

[1848] CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, *op. cit.*

[1849] *Idem*. Propos qu'elle avait déjà formulé dans CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », 19 juillet 2022, *op. cit.*, p. 4.

[1850] CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, *op. cit.*

[1851] *Idem*.

mise en œuvre de ce droit dans les cas où il entrerait en contradiction avec les finalités poursuivies[1852].

638. Aujourd'hui, les avis formulés par la CNIL concernant des technologies de sécurité publique font parfois face à l'incompréhension des différents acteurs (concepteurs et utilisateurs) qui la jugent trop sévère ou considèrent que son analyse évoque des situations trop hypothétiques[1853]. Les raisons pouvant expliquer cette discordance entre les autorités publiques et la CNIL pourraient résulter du manque de transparence et d'explicabilité des solutions technologiques développées (v. **n° 399 et suiv.**) tant s'agissant des personnes concernées que des AAI chargées d'assurer le respect des droits et des libertés. Pour autant, il ne faudrait pas reprocher à la CNIL son « excès » de vigilance car il se pourrait qu'elle soit aujourd'hui l'un des derniers remparts des droits et libertés face aux usages exponentiels de technologies de sécurité publique toujours plus intrusives et contraignantes. Outre ses quelques détracteurs, la CNIL se trouve depuis longtemps confrontée à une insuffisance de moyens, autant financiers que humains, en vue de remplir les missions qui lui ont été confiées et qui vont inévitablement s'amplifier avec l'arrivée des technologies augmentées[1854] (v. **n° 739 et suiv.**). En ce sens, la dernière affaire révélée par la presse concernant l'emploi d'un algorithme d'analyse d'images de vidéoprotection par les forces de l'ordre[1855], appelé *Briefcam*, démontre le besoin d'amplifier les moyens de la CNIL afin qu'elle puisse continuer à assurer un contrôle de tous les traitements de DACP.

2. Les limites au pouvoir de contrôle de la CNIL sur les technologies de surveillance de sécurité publique

639. Le renforcement de la protection des droits et libertés par les AAI repose sur la mise en œuvre de moyens tant humains que financiers. En ce sens, ces autorités appellent à l'octroi de

---

[1852] *Ibid*.

[1853] Voir en ce sens : BERTRAND (B.), « Encadrement des technologies de surveillance : les enseignements de l'expérimentation des JO 2024 », *op. cit.* (visioconférence) ; CNIL, « Caméras "augmentées" dans les espaces publics », *op. cit.* (webinaire).

[1854] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022, *op. cit.*, 4.2.3, pp. 200-203.

[1855] DESTAL (M.), LE FOLL (C.) et LIVOLSI (G.) « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », *Disclose*, 14 novembre 2023 [en ligne] : Ainsi, la presse a révélé l'existence d'un logiciel d'analyse d'images de vidéoprotection utilisé, essentiellement, à des fins de reconnaissance faciale par les forces de l'ordre en dépit de son interdiction par la législation en vigueur (loi JOP2024 d'expérimentation des caméras « augmentées »).

moyens supplémentaires[1856] afin de maintenir leur effectivité face à la demande croissante et aux nouvelles missions qui leur sont confiées. Elles requièrent le recrutement de personnes qualifiées dans des domaines de plus en plus précis afin notamment de faire face aux nouveaux enjeux et dispositions en matière d'algorithmes d'IA.

640. Aussi, la CNIL semble pâtir de moyens limités en comparaison de ceux octroyés à des autorités homologues en Allemagne et au Royaume-Uni[1857] (v. **n° 743-744**), ce qui suscite depuis longtemps l'inquiétude de ses présidents successifs[1858] à l'instar d'Alex Türk[1859]. En 2011, il exprimait de nouveau ses doutes quant aux capacités de la CNIL à assurer ses missions toujours plus nombreuses compte tenu des moyens encore insuffisamment mis en œuvre[1860]. Ces dernières années, la CNIL a vu ses compétences croître considérablement bien que les investissements nécessaires à l'exercice de ses missions semblent encore faire défaut. En ce sens, son champ de compétences s'est élargi à d'autres aspects que ceux propres à l'informatique à l'instar du contrôle des usages de la vidéosurveillance et de la vidéoprotection. En outre, elle doit aujourd'hui faire face aux multiples ramifications de ces systèmes de surveillance (caméras intelligentes, caméras mobiles, etc.). Néanmoins, l'entrée en vigueur du RGPD et de la DPJ, introduisant les principes de protection des données dès la conception (*privacy by design*) et de mise en conformité des traitements (*accountability*), s'est avérée salvatrice en vue de pallier le manque de moyens de la CNIL face aux besoins grandissants de mise en conformité aux règles de protection des DACP des organismes tant privés que publics. Aussi, la CNIL n'est pas seule dans son rôle de protectrice des droits et libertés puisque le Défenseur des droits participe également à leur garantie dans le cadre des usages technologiques.

1856 BONFORT (A.), COLIN (C.), DEBAETS (E.), SCHMITZ (J.), MARGUIN (J.), VIGNÉ (V.), PALMA-AMALRIC (V.) et MESTARI (Z.), « Autorités administratives indépendantes et libertés – actualités de l'année 2022 », *RDLF*, 27 mars 2023, chron. n° 20 [disponible en ligne].

1857 SAURON (J-L.), « Les autorités de contrôles de protection des données un point d'étape de leurs moyens et de leur pratique », *RLDI* n° 186, novembre 2021, pp. 36-41, spéc. p. 37.

1858 OBERDORFF (H.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 398.

1859 Propos du président de la CNIL Alex Türk dans : Rapport de l'office parlementaire d'évaluation de la législation n° 404 (2005-2006) sur « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié » remis par GÉLARD (P.), 15 juin 2006, p. 94 [en ligne].

1860 TÜRK (A.), *La vie privée en péril, des citoyens sous surveillance*, *op. cit.*, p. 201.

B. Le rôle du Défenseur des droits face aux technologies à l'usage des forces de l'ordre

641. Autorité administrative indépendante (AAI) instituée par deux lois du 29 mars 2011[1861] et citée par la Constitution depuis sa révision du 23 juillet 2008[1862], il fusionne plusieurs autres AAI[1863]. L'inscription du Défenseur des droits dans le texte de la Constitution lui confère une existence garantie constitutionnellement[1864]. Il a vocation à veiller « au respect des droits et libertés par les administrations de l'État, les collectivités territoriales, les établissements publics, ou à l'égard duquel la loi organique lui attribue des compétences »[1865]. En dépit des difficultés rencontrées lors du processus de fusion des différentes AAI et des craintes d'une régression des garanties qu'elles procuraient[1866], les efforts fournis par les représentants successifs du Défenseur des droits ont permis d'élever son rôle de gardien des droits et libertés[1867]. Il est même parfois qualifié de *human rights ombudsman*[1868] dont le rôle est de protéger, en toute indépendance[1869], les

---

[1861] Loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits, *JORF* n°0075 du 30 mars 2011 [en ligne] et Loi n° 2011-334 du 29 mars 2011 relative au Défenseur des droit, *JORF* n°0075 du 30 mars 2011 [en ligne] complétées par le Décret n° 2011-905 du 29 juillet 2011 relatif à l'organisation et au fonctionnement des services du Défenseur des droits, *JORF* n°0175 du 30 juillet 2011 [en ligne] et le Décret n° 2011-904 du 29 juillet 2011 relatif à la procédure applicable devant le Défenseur des droits, *JORF* n°0175 du 30 juillet 2011 [en ligne].

[1862] La loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la Ve République, *op. cit.*, a permis d'y introduire le Défenseur des droits mentionné à l'article 71-1.

[1863] Au rang des anciennes AAI concernées se trouve le Médiateur de la République, le Défenseur des enfants, la Haute Autorité de Lutte contre les Discriminations et pour l'Égalité (HALDE) et la Commission Nationale de Déontologie de la Sécurité (CNDS).

[1864] DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 83.

[1865] Constitution de 1958, art. 71-1.

[1866] Voir notamment en ce sens : Propos de GOULARD (F.) dans AN, Séance du 29 mai 2008, *JOAN* du 30 mai 2008, n° 41, p. 2711 ; Propos de BADINTER (R.) dans Sénat, Séance du 24 juin 2008, *JO Sénat* du 25 juin 2008, n° 51, p. 3392.

[1867] LOHRER (D.), « Le défenseur des droits : quel bilan après dix ans d'activité ? », *RFDA*, janvier-février 2021, étude pp. 73-86, spéc. p. 73 : « Dominique Baudis d'abord […] Jacques Toubon ensuite qui poursuivant l'œuvre fondatrice engagée par son prédécesseur, a su convaincre par sa rigueur et son obstination. Claire Hédon enfin issue de la société civile et connue pour son engagement en faveur des droits fondamentaux ». Voir notamment : « 20 MINUTES AVEC... » Jacques Toubon, *20minutes.fr*, 12 juin 2020 [en ligne] où il avait exprimé son inquiétude « de voir que des mesures prises dans le cadre de l'état d'urgence sanitaire et qui se doivent d'être temporaires, soient inscrites de manière permanente dans la loi. C'est ce qui s'est produit en 2017 avec la loi sur la sécurité intérieure pour quatre mesures de l'état d'urgence antiterroriste ».

[1868] Voir en ce sens : *Ibid* ; DENIZEAU (C.), *Droit des libertés fondamentales*, *op. cit.*, p. 82 ; AUTIN (J-L.), « Fasc. 75 Les autorités administratives indépendantes », *JCl. Administratif*, 20 juillet 2010, màj le 3 janvier 2022, § 34 ; YOUHNOVSKI SAGON (A-L.), « Les recommandations du Défenseur des droits : un couteau suisse au service du respect des droits et libertés fondamentaux », *Droit administratif* n° 11, novembre 2022, étude 12 : « le Défenseur des droits constitue le seul *ombudsman* possédant une compétence générale et spécialisée dans [le] domaine » de la défense des droits et libertés.

[1869] Si l'indépendance du Défenseur des droits a parfois pu être questionnée (voir notamment : HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 272), ses représentants ont su en faire la démonstration au cours de ses dix années d'existence (voir pour exemple : DDD, Rapport annuel d'activité 2018, p. 2 [en ligne] et DDD, Rapport annuel d'activité 2019, p. 5 [en ligne]).

droits et libertés par l'intermédiaire de son pouvoir de recommandation. Au sein des institutions non-juridictionnelles, le Défenseur des droits endosse aussi un rôle important de garant des droits et libertés face aux moyens technologiques mis à la disposition des pouvoirs publics.

642. Les prérogatives du Défenseur des droits - Face aux insuffisances que peuvent présenter les garanties juridictionnelles, en raison de leur intervention *a posteriori*, le Défenseur des droits se présente comme une solution complémentaire intéressante par son pouvoir de recommandation[1870]. En vue de prévenir et de faire cesser les atteintes portées aux droits et libertés, le législateur lui a conféré une pluralité de pouvoirs dont celui de prévention du contentieux, d'une part, et de règlement alternatif des litiges, d'autre part. Ce pouvoir de résolution des différends s'assimile à une procédure de conciliation dans la mesure où le Défenseur conserve un rôle neutre en se tenant à la formulation de propositions visant à mettre fin aux agissements portant atteinte aux droits et libertés. Néanmoins, lorsque ses recommandations ne sont pas suivies d'effets, le Défenseur peut exercer son pouvoir d'injonction qui constitue une « obligation procédurale »[1871], en d'autres termes, une contrainte non coercitive assimilable à une obligation de moyens en vue de faire exécuter les recommandations formulées[1872]. Dès lors, les recommandations du Défenseur ont une vocation incitative. L'absence de suite donnée à son injonction l'autorise à rédiger un rapport spécial, à l'attention du destinataire de la recommandation, qui peut être mis en ligne, ce que le Défenseur qualifie « d'interpellation publique »[1873], en vue de faire connaitre les comportements ou pratiques illicites d'une personne (physique ou morale) ou d'une administration[1874].

643. Le Défenseur des droits endosse un rôle essentiel en matière de prévention des atteintes aux droits et libertés, notamment en attirant l'attention du législateur sur les différentes menaces pouvant peser sur eux[1875]. À titre d'exemple, l'actuelle Défenseure, Claire Hédon, avait souligné les

---

[1870] Le pouvoir de recommandation est décrit par l'article 25 de la loi organique n° 2011-333 du 29 mars 2011, *op. cit.*, comme ayant pour objectif de « garantir le respect des droits et libertés de la personne lésée et à régler les difficultés devant lui ou à en prévenir le renouvellement ».

[1871] MOUCHETTE (J.), *La magistrature d'influence des autorités administratives indépendantes*, Paris, LGDJ, Thèse, 2019, 714 p., p. 592.

[1872] Voir en ce sens : C. const., Décision n° 87-237 DC, 30 décembre 1987, *Loi de finances pour 1988*, Rec. p. 63 [en ligne] ; C. const., Décision n° 88-248 DC, 17 janvier 1989, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*, Rec. p. 18 [en ligne].

[1873] DDD, Rapport annuel 2011, p. 24 [en ligne].

[1874] MOUCHETTE (J.), *La magistrature d'influence des autorités administratives indépendantes*, *op. cit.*, p. 236.

[1875] DDD, Rapport annuel d'activité 2018, *op. cit.*, p. 2.

nombreuses atteintes possibles au droit à la vie privée ainsi qu'à la protection des DACP que présentait le recours à des drones aériens[1876]. Le Défenseur des droits peut formuler des recommandations de portée individuelle et de portée générale. Les recommandations de portée générale sont des propositions de réformes législatives, réglementaires ou administratives qui paraissent nécessaires à mettre en œuvre[1877]. Outre ses études et rapports, le Défenseur fait appel aux réclamations qui lui sont adressées pour formuler des propositions de réformes les plus concrètes au regard des situations du quotidien et des travaux effectués par les juristes dans le domaine concerné[1878].

644. Dans le cadre de l'exercice de ses missions, le Défenseur des droits n'hésite pas à faire usage de son droit d'adresser des observations devant les juridictions civiles, pénales et administratives[1879] qui sont, par ailleurs, en grande partie suivies par les juges[1880]. Aussi, il entretient des rapports positifs avec les autres AAI chargées d'assurer la protection des droits et libertés au nombre desquelles la CNIL, comme en témoignent les renvois de ses avis[1881]. Par ailleurs, il collabore avec la CEDH et souhaite contribuer à l'application effective de ses arrêts par l'État français[1882]. Enfin, le Défenseur des droits dispose également d'une expertise et de prérogatives essentielles à la protection des droits et libertés lui permettant d'apporter sa contribution au contrôle de constitutionnalité des lois. Pour ce faire, il peut soumettre des observations au Conseil constitutionnel (lors d'un recours en inconstitutionnalité *a priori*), d'une part, et appuyer l'envoi d'une question prioritaire de constitutionnalité lorsqu'il intervient devant une juridiction suprême, d'autre part[1883].

[1876] DDD, avis n°20-05 du 3 novembre 2020, *op. cit.*, p. 3.

[1877] Dans le cadre de son rôle consultatif, le Défenseur des droits peut formuler des propositions des textes législatifs et réglementaires dans son rapport annuel (HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, *op. cit.*, p. 274).

[1878] YOUHNOVSKI SAGON (A-L.), « Les recommandations du Défenseur des droits : un couteau suisse au service du respect des droits et libertés fondamentaux », *op. cit.*

[1879] Loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits, *op. cit.*, art. 33.

[1880] LOHRER (D.), « Le défenseur des droits : quel bilan après dix ans d'activité ? », *op. cit.*, p. 76.

[1881] À titre d'exemple : DDD, avis n°20-06 du 17 novembre 2020, *op. cit.*, p. 4 (caméras piéton) ; DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*, p. 5 (caméras filmant la garde à vue) et pp. 7-8 (caméras aéroportées).

[1882] DDD, Rapport annuel 2011, *op. cit.*, p. 30 et p. 143.

[1883] LOHRER (D.), « Le défenseur des droits : quel bilan après dix ans d'activité ? », *op. cit.*, p. 79.

645. Les limites subsistantes du rôle du Défenseur des droits - Le Défenseur des droits présente toutefois toujours des lacunes d'efficacité mais il semblerait que certains des obstacles auxquels il faisait face se résorbent progressivement. En premier lieu, son efficacité peine encore parfois à convaincre, une grande partie de ses propositions de réformes n'étant pas prises en compte lors de l'élaboration des textes législatifs[1884]. La raison reposerait vraisemblablement sur l'absence de pouvoir de contrainte du Défenseur des droits[1885], celui-ci ne disposant que d'un pouvoir d'injonction comme moyen de faire « pression » sur les pouvoirs publics. S'il peine encore à convaincre ces derniers, il peut néanmoins se satisfaire de sa saisine en matière de contentieux qui est en constante croissance[1886] même si elle demeure en deçà des espoirs formulés par le précédent Défenseur[1887]. Toutefois, il pâtit toujours (au même titre que d'autres AAI) d'une insuffisance de moyens financiers et humains qui ne lui permet pas d'assurer un suivi des dossiers dans des délais adaptés[1888].

646. Les technologies de sécurité publique sous le regard du Défenseur des droits - Parmi les nombreux sujets que traite le Défenseur des droits, celui des moyens technologiques à l'usage des forces de l'ordre fait l'objet d'avis et d'études approfondies quant à leur incidence sur le respect des règles de déontologie de la sécurité, du droit à la vie privée ou encore du principe de non-discrimination[1889]. Ainsi, il considère comme acquis le recours à des moyens tels que la mise en œuvre de caméras fixes de vidéoprotection[1890] sous réserve qu'elle s'effectue « conformément à un strict cahier des charges »[1891]. En revanche, le Défenseur des droits ne considère pas leur usage comme anodin et a émis plusieurs réserves s'agissant d'autres outils technologiques à l'usage des

---

[1884] Voir en ce sens les rapports annuels d'activité du Défenseur des droits.

[1885] LOHRER (D.), « Le défenseur des droits : quel bilan après dix ans d'activité ? », *op. cit.*, p. 84.

[1886] Le rapport annuel d'activité de 2022 faisait ainsi état d'une augmentation de 9% des saisine par rapport à l'année 2021 (DDD, Rapport annuel d'activité 2022 [en ligne]).

[1887] « À la veille de son départ, le Défenseur des droits encourage les Français à saisir l'institution », *Le Figaro*, 1er juillet 2020 [en ligne] : « Je voudrais que le Défenseur en traite 500.000 [demandes] » par an.

[1888] Voir les différents rapports annuels du Défenseur des droits.

[1889] Voir notamment : DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020, *op. cit.* ; DDD, avis n°20-13 du 21 décembre 2020, *op. cit.* ; DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*

[1890] DDD, avis n°20-13 du 21 décembre 2020, *op. cit.*, p. 3 ; DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*, p. 6.

[1891] NICOUD (F.), « Le Défenseur des droits et la sécurité », p. 68 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 61-70.

forces de l'ordre tels que les drones aériens[1892] et ceux reposant sur des algorithmes d'IA (ex. reconnaissance faciale, algorithmes de « police prédictive », etc.)[1893]. S'il a reconnu l'utilité de ces moyens dans le cadre des missions de prévention et de répression des atteintes à l'ordre public, il s'est inquiété des possibilités que l'emploi de technologies reposant sur des algorithmes puisse induire des discriminations[1894].

647. Dans son rapport de mai 2020, il avait indiqué que ces technologies présentaient encore des limites et que leurs résultats n'étaient pas neutres en raison de leur conception reposant principalement sur des « données reflétant des pratiques humaines »[1895]. Dans son avis du 17 novembre 2020 sur la proposition de loi relative à la sécurité globale, le Défenseur avait soulevé des réserves quant à l'emploi de drones aériens par les forces de l'ordre, considérant qu'ils présentaient de nouveaux moyens d'atteinte à la vie privée dans la mesure où le texte n'offrait pas suffisamment de garanties[1896]. Dans son avis du 20 septembre 2021 relatif au projet de loi RPSI, il avait reconnu les améliorations des dispositions portant sur les drones aériens en comparaison de celles de la loi pour une sécurité globale mais avait néanmoins noté encore plusieurs lacunes pouvant limiter la protection du droit à la vie privée[1897]. En outre, rejoignant l'avis de la CNIL[1898], il avait reproché au texte de présenter des finalités trop « générales et peu circonstanciées »[1899] allant à l'encontre d'un usage limité nécessaire pour justifier leur utilisation. Dès lors, il avait insisté sur la nécessité pour les agents des forces de l'ordre de faire un usage « contrôlé » de ces différents moyens technologiques. Néanmoins, il est regrettable que ses observations n'aient, là encore, pas été suffisamment prises en considération lors de l'élaboration de la loi RPSI. Il semblerait toutefois que ses inquiétudes concernant le traitement de certaines DACP sensibles (telles que la biométrie

---

[1892] DDD, avis n°20-05 du 3 novembre 2020, *op. cit.*, p. 3 ; DDD, avis n°20-06 du 17 novembre 2020, *op. cit.*, spéc. pp. 4-5 ; DDD, avis n°20-13 du 21 décembre 2020, *op. cit.*, spéc. pp. 3-4 ; DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*, spéc. pp. 6-9.

[1893] DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », 19 juillet 2019, *op. cit.* ; DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020, *op. cit.* ;

[1894] NICOUD (F.), « Le Défenseur des droits et la sécurité », p. 69 *in* GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, *op. cit.*, pp. 61-70.

[1895] DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020, *op. cit.*, p. 6.

[1896] DDD, avis n°20-06 du 17 novembre 2020, *op. cit.*, spéc. p. 5.

[1897] DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*, p. 7 : « Le projet de loi apporte des garanties par rapport au texte censuré par le Conseil constitutionnel « pour autant « l'encadrement ne semble […] pas suffisamment strict alors que les possibilités d'utilisation des images prises par les caméras aéroportées sont nombreuses ».

[1898] CNIL, Délibération n° 2021-011 du 26 janvier 2021, avis n° 20020769, *op. cit.*

[1899] DDD, avis n°21-12 du 20 septembre 2021, *op. cit.*, p. 7.

faciale) par des algorithmes d'analyse d'image et des risques de discrimination eut un écho auprès des membres du Parlement[1900].

648. Le Défenseur des droits a su démontrer ses qualités de garant mais ses recommandations nécessitent d'être davantage prises en considération afin d'assurer une protection effective des droits et libertés à l'heure où les drones aériens de sécurité publique s'équipent progressivement de logiciels d'analyse d'images.

[1900] Voir : Loi JOP2024 (exclue tout forme de traitement de données biométriques par les caméras équipés d'algorithmes d'analyse d'images) ; Sénat, Rapport d'information n° 627 (2021-2022), 10 mai 2022, *op. cit.* (analyse les conséquences d'une utilisation de caméras « augmentées » traitant des données biométriques, principalement le visage).

CONCLUSION DU TITRE I

649. Le recours aux technologies de surveillance « augmentées » repose sur une volonté d'améliorer la sécurité des personnes et de leurs biens. Néanmoins, ainsi que l'affirme la Commission nationale consultative des droits de l'Homme, il est à déplorer que « tout se passe comme si la simple invocation d'une plus grande efficacité pouvait justifier l'adoption, sans aucune discussion, des mesures les plus attentatoires aux libertés »[1901]. En ce sens, la professeure Danièle Lochak rappelle que cette sécurité a un prix, celui d'exercer « de nouvelles formes de surveillance, moins pesantes, parce que moins visibles, mais plus sournoises, plus indiscrètes, et finalement plus attentatoires à la liberté individuelle et à la vie privée »[1902]. Aussi, la professeure Véronique Champeil-Desplats fait remarquer qu' « aucun mécanisme juridique - pas même le juge -, aucun levier économique, aucune politique publique n'offrent en eux-mêmes une solution imparable, universelle et définitive » et qu'il est donc nécessaire de « penser non seulement leur adéquation aux fins poursuivies mais aussi leur modalité de coordination »[1903]. Dès lors, les technologies de surveillance « augmentées » nécessitent un cadre juridique adapté à leurs enjeux.

650. Les différentes institutions juridictionnelles nationales et internationales ont toujours été présentées comme les premières garantes de la protection des droits et libertés[1904]. Pourtant, les évolutions technologiques, notamment en matière de sécurité publique, tendent à démontrer qu'elles ne sont plus les seules à assurer cette fonction depuis l'arrivée des institutions non-juridictionnelles chargées également de protéger les droits et libertés[1905]. Si les juridictions internes, confrontées aux exigences sociales de sécurité, tendent à s'enliser dans leur devoir de défense des droits et libertés, les juges européens œuvrent davantage à leur protection. Mais, face aux contraintes juridictionnelles, les AAI, à commencer par la CNIL, pourraient bien offrir des solutions plus adaptées pour autant que des moyens suffisants soient mis à leur disposition.

1901 CNCDH, Avis sur le projet de loi relatif au renseignement, 16 avril 2015, *JORF* n°0171 du 26 juillet 2015 texte n°43 [en ligne].

1902 LOCHAK (D.), *Les droits de l'homme*, Paris, La Découverte, coll. Repères, 4ème édition, 2018, 128 p., p. 106.

1903 CHAMPEIL-DESPLATS (V.), *Théorie générale des droits et libertés*, *op. cit.*, p. 304.

1904 LEBRETON (G.), *Libertés publiques et droits de l'homme*, *op. cit.*, p. 214 : Les garanties juridictionnelles constituent « le rempart le plus efficace ».

1905 YOUHNOVSKI SAGON (A-L.), « Les recommandations du Défenseur des droits : un couteau suisse au service du respect des droits et libertés fondamentaux », *op. cit.* : « Le développement de modes de protection non-juridictionnelle participe à la fortification » de la protection des droits et libertés.

TITRE II LES PERSPECTIVES DE RENFORCEMENT DE LA PROTECTION DES DROITS ET LIBERTÉS FACE AUX TECHNOLOGIES DE SURVEILLANCE « AUGMENTÉES » DE SÉCURITÉ PUBLIQUE

651. L'ensemble des développements qui précède incite à l'encadrement du recours aux technologies de surveillance « augmentées » de sécurité publique plutôt qu'à une ferme et vaine opposition aux développements inéluctables du domaine. De fait, l'usage des technologies « augmentées » à des fins de sécurité publique présente des opportunités qui ne peuvent être ignorées. Ces technologies pourraient apporter un réel bénéfice aux forces de l'ordre ainsi qu'aux services de secours. Néanmoins, les perspectives d'amélioration des missions de sécurité publique qu'offrent les technologies « augmentées » nécessitent, en contrepartie, un renforcement du cadre juridique tant national que supranational. Plusieurs instruments juridiques existent pour encadrer le développement et l'usage des technologies « augmentées » mais ne suffisent plus à garantir de manière effective la protection des droits et libertés. Aussi, de nombreux acteurs ont travaillé au développement de solutions techniques, juridiques et éthiques afin de résoudre certains enjeux spécifiques aux technologies « augmentées » (**Chapitre 1**).

652. Le recours aux technologies de surveillance « augmentées » par les forces de l'ordre conduit à une limitation des droits et libertés légitimée par des besoins de sauvegarde de l'ordre public. Pour autant, la légitimité des mesures de police n'est acquise que sous réserve de respecter un principe de de proportionnalité et de nécessité. Ce principe, consacré par la jurisprudence française et européenne, conditionne l'adoption des dispositions législatives. Le Conseil constitutionnel assure le contrôle du respect de ce principe dans le cadre de sa procédure d'examen de la constitutionnalité des textes législatifs. Face aux usages technologiques des forces de l'ordre, le principe de proportionnalité et de nécessité se présente comme un rempart des droits et libertés. Cependant, la pression exercée par les politiques sécuritaires a eu une incidence sur les décisions du Conseil constitutionnel et tend à affaiblir la portée de ce principe (**Chapitre 2**).

CHAPITRE 1 UN RENOUVELLEMENT DES GARANTIES POUR LA PROTECTION DES DROITS ET LIBERTÉS

653. Il serait autant contre-productif que naïf de vouloir s'opposer aux développements technologiques même dans un cadre aussi sensible que celui du régalien. Le professeur Henry Oberdorff constatait en ce sens que plutôt que d'empêcher toute forme de progrès technologique pour se prémunir des éventuelles conséquences néfastes, la solution majoritairement adoptée était celle d'un accompagnement et d'un encadrement des évolutions technologiques à l'échelle des différents acteurs[1906]. L'ensemble des acteurs semble donc s'accorder pour construire un environnement propice au développement et au recours aux SIA qui respecterait des principes juridiques et éthiques[1907]. Néanmoins, les moyens pour y parvenir ne font pas toujours l'unanimité. Certains acteurs souhaitent interdire certaines formes de SIA qu'ils estiment être porteurs d'atteintes disproportionnées aux droits et libertés[1908]. D'autres acteurs s'opposent à l'idée même de mettre en œuvre une réglementation générale des SIA considérant qu'elle briderait l'innovation[1909]. D'une manière générale, une majorité d'acteurs a formulé le souhait d'adopter un cadre juridique adapté aux développements et aux usages des SIA qui renforcerait les garanties protégeant les droits et libertés[1910] (**Section 1**).

654. Aussi, le renforcement des garanties protégeant les droits et libertés ne peut se contenter de la mise en œuvre de normes juridiques et nécessite « la maitrise consciente du développement technologique »[1911] par tous les acteurs, privés comme publics. La « maîtrise » des technologies de surveillance « augmentées » de sécurité publique suppose l'adoption de mesures tant juridiques que

---

[1906] OBERDORFF (H.), « Le droit, la démocratie et la maitrise sociale des technologies », *RDP*, 1992, p. 983.

[1907] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 123.

[1908] REIA, art. 5 ; EDPB, Avis conjoint 05/2021 concernant la législation sur l'intelligence artificielle, *op. cit.*, pp. 12-14 §§ 27-35 ; Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*, notamment § 26 ; CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, *op. cit.*, pp. 9-15 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, pp. 73-77.

[1909] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 326 ; JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 123.

[1910] De manière non-exhaustive : Rapport VILLANI, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne », *op. cit.*, spéc. pp. 150-152 ; REIA ; EDPB, Avis conjoint 05/2021 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.* ; Sénat, Rapport d'information n° 627, *op. cit.* ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*

[1911] TOFFLER (A.), *Le choc du Futur*, éd. Denoël, 1971, 539 p., pp. 447-478.

techniques permettant d'en comprendre le fonctionnement et d'en assurer le déploiement garantissant le maintien de la souveraineté ainsi que le respect des droits et libertés (**Section 2**).

Section 1 Un socle juridique pour encadrer les technologies de surveillance « augmentées » de sécurité publique

655. L'introduction des technologies « augmentées » au sein de la sphère publique incite à une certaine méfiance[1912] qui s'explique majoritairement par un manque de compréhension de leur fonctionnement. Aussi, la multiplicité des enjeux qu'elles engendrent pour les droits et libertés constitue un frein à leur acceptabilité sociétale. Le recours à ces technologies par les pouvoirs publics appelle donc la mise en œuvre d'un cadre juridique adapté[1913]. En ce sens, le Conseil d'État rappelait que « les pouvoirs publics ont […] la responsabilité de définir les conditions et les garanties de l'IA de confiance dans le secteur public - qui s'imposeront tant aux acteurs publics qu'aux acteurs privés en tant qu'ils fournissent des SIA aux administrations »[1914]. L'élaboration de ce cadre juridique suppose néanmoins de repenser la manière de concevoir les textes juridiques en impliquant davantage d'acteurs. Les travaux issus des réflexions scientifiques et doctrinales apportent de premières réponses sur les conditions et les moyens à mettre en œuvre en vue d'assurer une maîtrise des risques et des limitations que présentent les technologies « augmentées » de sécurité publique pour les droits et libertés.

[1912] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 16 : « Dans un certain imaginaire collectif, la force publique porte en elle des risques de dérive sécuritaire. La méfiance et la défiance que ressent une partie de la population envers l'État et la fonction de sécurité qui lui est confiée, nourrissent ces craintes. Elles interviennent dans un contexte où est largement répandu le sentiment que les droits et libertés fondamentaux tendent à reculer » ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 93 : Le Conseil d'État formulait le constat d'une « méfiance naturelle qu'inspire le recours à des machines et à des technologies souvent mal comprises » ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 4 : « la perspective d'une surveillance et d'une analyse algorithmique permanentes d'espaces publics peut générer ainsi de fortes inquiétudes ».

[1913] Rapport VILLANI, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne », *op. cit.*, spéc. pp. 151-152.

[1914] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 94.

656. Ainsi, plusieurs institutions nationales[1915] et européennes[1916] appellent de leurs vœux l'adoption de principes généraux communs aux SIA, qui seraient applicables aux technologies « augmentées » de sécurité publique, au sein d'une règlementation générale des SIA. Cette réglementation, représentée par le REIA issu des travaux de la Commission et du Parlement européens, apportera une première réponse à l'encadrement des SIA mais devra être complétée par des dispositions nationales afin d'encadrer plus spécifiquement les différents usages suivant les secteurs d'activité, les finalités ainsi que les types de données collectées (§1). Néanmoins, la garantie effective des dispositions réglementaires doit s'accompagner de mesures de contrôle tant techniques que juridiques afin de s'assurer que les SIA respectent les principes protecteurs des droits et libertés tout au long de leur cycle de vie (§2).

§1. Un cadre juridique adapté aux technologies de surveillance « augmentées » pour garantir la protection des droits et libertés

657. Un encadrement effectif des technologies de surveillance « augmentées » de sécurité publique suppose la mise en œuvre de dispositions contraignantes, dites de droit dur, qui peuvent s'accompagner de dispositions non contraignantes, dites de droit souple, telles que les normes[1917]. À cet effet, le REIA comprend plusieurs dispositions énonçant des principes généraux communs à tous les SIA dont certains sont similaires à ceux présents au sein de la réglementation relative à la protection des DACP. De même, la Convention sur l'IA que souhaite adopter le Conseil de l'Europe entend également encadrer juridiquement le développement et l'usage de l'IA. Néanmoins, l'élaboration d'un cadre général des SIA ne suffit pas et les technologies de surveillance

---

[1915] CNIL, « Comment permettre à l'homme de garder la main ? : Les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.* ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, spéc. pp. 43-47 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, spéc. pp. 98-134 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., spéc. pp. 77-78 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, spéc. pp. 11-14.

[1916] Conseil de l'Europe, « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ), 3-4 décembre 2018, *op. cit.*, spéc. pp. 8-12 ; Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », *op. cit.*, spéc. §§ 17-22 ; REIA. Il semble également opportun d'ajouter la « Convention [cadre] sur la conception, le développement et l'utilisation des systèmes d'intelligence artificielle qui se fonde sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit et est propice à l'innovation, conformément aux décisions pertinentes du Comité des Ministres » en cours de rédaction par le Comité sur l'Intelligence artificielle du Conseil de l'Europe [Voir : en ligne].

[1917] Voir à ce sujet : HO-DAC (M.), « La normalisation, clé de voûte de la règlementation européenne de l'intelligence artificielle (*AI Act*) », *Dalloz IP/IT* n° 4, 20 avril 2023, p. 228.

« augmentées » de sécurité publique nécessitent l'adoption d'une législation nationale adaptée à leurs différents cas d'usage[1918] (A). Aussi, l'acceptabilité sociétale du recours à ces technologies par les autorités publiques requière également l'adoption de dispositions permettant l'application du droit au recours effectif par les personnes sujettes des décisions relevant pour part des résultats du SIA (B).

A. Des normes juridiques applicables aux technologies de surveillance « augmentées » de sécurité publique

658. L'adoption de dispositions juridiques et techniques contraignantes est autant un gage de confiance à l'égard des SIA qu'un moyen d'assurer leur déploiement par les différents acteurs dans le respect des droits et libertés[1919]. Compte tenu de leurs effets, les SIA nécessitent un encadrement juridique spécifique reposant sur des règles et des principes généraux communs (1). Au-delà des règles régissant la protection des DACP et des principes généraux formulés par les institutions européennes, le recours aux technologies de surveillance « augmentées » de sécurité publique appelle la mise en œuvre d'un cadre juridique national adapté à chaque cas d'usage[1920] privilégiant la mise en œuvre d'une phase expérimentale sous la forme d'une législation temporaire[1921] (2).

1. Les règles et principes généraux communs à l'usage des technologies de surveillance « augmentées » de sécurité publique

659. Dans la mesure où les technologies de surveillance « augmentées » de sécurité publique « captent et analysent des données, en particulier des images qui permettent d'identifier des personnes »[1922], leur recours constitue un traitement de DACP. Dès lors, même si les DACP

[1918] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, spéc. pp. 14-16.

[1919] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 134.

[1920] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, pp. 14-16.

[1921] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 46-47 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., spéc. pp. 79-82.

[1922] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 11.

collectées ont vocation à être supprimées dans un bref délai après leur collecte[1923], les concepteurs et les utilisateurs de ces technologies devront appliquer les exigences relatives à la protection des DACP. En ce sens, la règlementation afférente à la protection des DACP présente un intérêt majeur en ce qu'elle consacre des principes et des garanties qui s'appliquent à l'utilisation des technologies « augmentées »[1924] (a). Aussi, un socle juridique permettant le recours à des technologies de surveillance « augmentées » de sécurité publique suppose l'application de principes et exigences communs en vue de permettre leur expérimentation dans un cadre clair, d'une part et, leur usage dans le respect du principe de proportionnalité, d'autre part[1925]. Certains principes sont déjà formulés par la réglementation relative à la protection des DACP[1926]. Néanmoins, d'autres exigences et principes que ceux afférents à la protection des DACP, et qui s'inspirent des principes issus de l'éthique[1927], doivent être mis en œuvre afin d'encadrer les SIA. À cette fin, le REIA repose sur un certain nombre de principes généraux communs qui ont été dégagés par plusieurs institutions, tant nationales que supranationales, afin d'assurer une conception et un usage de l'ensemble des SIA garantissant la protection des droits et libertés (b).

a. Le droit des DACP, support des premières mesures d'encadrement des technologies de surveillance « augmentées » de sécurité publique

660. Les technologies de surveillance « augmentées » de sécurité publique reposent sur un apprentissage et un fonctionnement nécessitant le traitement de données. Dans la mesure où une grande partie de ces données sont des DACP, l'emploi de ces technologies engendre *de facto* des

---

[1923] *Ibid* : « Même dans le cas où les images sont anonymisées, voire détruites, très rapidement après leur captation et analyse, ces opérations constituent un traitement de données à caractère personnel si les images contiennent des personnes ». En ce sens : CNIL, Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense (demande d'autorisation n° 1833589) [en ligne] dont la position fut confirmée plus tard par le Conseil d'État (CE, 10ème-9ème ch. réunies, 8 février 2017, n° 393714 [en ligne]) ; CE, ord., 18 mai 2020, *op. cit.* (sur la surveillance par drones aériens de la Préfecture de police de Paris).

[1924] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 12 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, Annexe 10, p. 347 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 242.

[1925] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 43.

[1926] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 74.

[1927] De manière non-exhaustive : Commission européenne, « Lignes directrices en matière d'éthique pour l'IA », *op. cit.* ; Parlement européen, « Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes », *op. cit.* ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, spéc. pp. 203-215.

effets sur la vie privée des personnes concernées. Dès lors, les responsables de traitement (concepteurs et utilisateurs) doivent se conformer aux différents textes juridiques qui consacrent un droit à la protection de la vie privée et des DACP.

661. Le cadre juridique protégeant les DACP - Plusieurs textes nationaux et supranationaux permettent de garantir le droit à la vie privée et la protection des DACP. Le droit à la vie privée fait l'objet d'une protection étendue à commencer par l'article 2 de la DDHC[1928] ainsi que par l'article 9 du Code civil[1929]. Au niveau européen, l'article 8 de la Conv.EDH permet de protéger la vie privée des individus contre les ingérences arbitraires de l'État et oblige celui-ci à en assurer la protection contre les tiers. De même, les articles 7 et 8 de la CDFUE consacrent un droit à la protection de la vie privée. En matière de protection des DACP, la LIL a permis de mettre en œuvre les premières mesures visant à assurer la protection des données des citoyens face aux évolutions technologiques. Elle se distingue par l'ouverture de ses dispositions qui lui permettent, encore aujourd'hui, d'intégrer les multiples évolutions technologiques[1930]. Elle précède les textes emblématiques européens en matière de protection des DACP (Directive de 1995 puis RGPD et DPJ) qui auront eu le mérite d'établir un cadre juridique unifié en la matière. Enfin, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe[1931], dite Convention 108, constitue le seul instrument juridique contraignant de niveau international en matière de protection des données personnelles[1932]. La modernisation du texte en 2018 a permis d'intégrer les évolutions technologiques en matière

---

[1928] En dépit du fait que le droit à la vie privée ne soit pas inscrit dans les textes constitutionnels (MAZEAUD (V.), « La constitutionnalisation du droit au respect de la vie privée », *Les nouveaux cahiers du Conseil constitutionnel* n° 48, juin 2015), le Conseil constitutionnel rattache la protection et le caractère de principe fondamental au droit à la vie privée à l'article 2 de la DDHC (C. const., Décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, *op. cit.*, cons. 45.

[1929] Pour rappel énonce que : « Toute personne a droit au respect de sa vie privée » (C. civ., art. 9). Le droit à la vie privée est également consacré par la jurisprudence de la Cour de cassation qui accorde un sens large à ce droit estimant que : « le droit de chacun au respect de sa vie privée s'étend à la présentation interne des locaux constituant le cadre de son habitat et, d'autre part, que l'utilisation faite des photographies qui en sont prises demeure soumise à l'autorisation de la personne concernée » (C. cass., 1ère civ., 7 novembre 2006, n° 05-12788 [en ligne]).

[1930] La LIL a néanmoins été plusieurs fois complétée et modifiée afin d'intégrer notamment les dispositions issues du RGPD (Loi n° 2018-493 du 20 juin 2018, *op. cit.*).

[1931] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite Convention 108), Strasbourg, 28 janvier 1981, 9 p. [en ligne].

[1932] De fait, elle est la seule Convention à laquelle les États non-membres du Conseil de l'Europe peuvent adhérer.

d'algorithmes et d'IA intégrant la prise de décisions automatisées[1933] ainsi qu'à aligner ses dispositions sur celles du RGPD en introduisant des exigences de transparence et de responsabilité[1934].

662. Les conditions aux traitements de DACP - Ces textes prévoient plusieurs garanties à la protection des DACP en imposant le respect de plusieurs principes et conditions aux fins d'effectuer un traitement de DACP[1935]. Ainsi, les responsables de traitements des technologies de surveillance « augmentées » de sécurité publique seront soumis à plusieurs obligations. Les données permettant d'identifier directement ou indirectement une personne, y compris par individualisation, doivent respecter des exigences légales. À cette fin, le responsable de traitement doit définir préalablement à tout traitement de DACP les finalités poursuivies, qui nécessitent d'être déterminées, explicites et légitimes[1936]. Aussi, il convient de distinguer les résultats qui seront produits par l'algorithme d'aide à la prise de décision de l'objectif qui constitue la finalité du traitement de DACP. Dans le cadre du recours à des drones aériens « augmentées » de sécurité publique dont l'algorithme aurait vocation à analyser et détecter les mouvements de foule, la finalité du traitement serait la prévention des atteintes aux personnes et non la détection *per se*. De même, un algorithme qui permettrait le suivi d'individus (via des données biométriques ou non) aurait pour finalité la recherche des auteurs d'infractions.

663. Le SIA ne peut effectuer un traitement de DACP que sur une base légale déterminée au cas par cas[1937]. Dans le cadre d'un usage de sécurité publique, la licéité du traitement de DACP est justifiée par la nécessité que suscite l'exécution d'une mission d'intérêt public[1938] ou relevant de

---

[1933] Conseil de l'Europe, Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 10 octobre 2018, 19 p. [en ligne]. La France a ratifié l'amendement de la Convention le 27 mars 2023 (CNIL, « La France ratifie la Convention 108+ du Conseil de l'Europe », *cnil.fr*, 30 mars 2023 [en ligne] consulté le 3 avril 2023).

[1934] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 21.

[1935] Les principes généraux relatifs à la protection des DACP sont énoncés par l'article 5 du RGPD et 4 de la DPJ.

[1936] RGPD, art. 5 §1 b) et DPJ, art. 4 §1 b).

[1937] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p.12.

[1938] RGPD, art. 6 §1 e).

l'exercice de l'autorité publique[1939]. Aussi, dans le cadre des drones aériens « augmentés » de sécurité publique, les DACP collectées par les forces de l'ordre ne peuvent faire l'objet d'un traitement à des fins autres que celles de « prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[1940]. En outre, les traitements de DACP entrant dans le cadre de la DPJ doivent faire l'objet d'une disposition juridique nationale précisant *a minima* « les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement »[1941].

664. Un recours proportionné aux SIA de sécurité publique - Le responsable du traitement de DACP devra démontrer, préalablement au recours à une technologie de surveillance « augmentée » de sécurité publique, la nécessité et la proportionnalité de ce traitement comme étant adapté à la base légale retenue. En outre, cette démonstration sera nécessaire lors de l'accomplissement de l'analyse d'impact relative à la protection des DACP[1942]. Dès lors, le responsable de traitement devra établir la nécessité d'avoir recours à une technologie de surveillance « augmentée ». L'évaluation de la nécessité du traitement repose sur deux conditions. D'une part, elle permet de déterminer l'existence ou non d'autres moyens moins intrusifs afin d'atteindre les finalités envisagées. D'autre part, elle permet d'effectuer une analyse « de l'utilité et de la performance opérationnelle du dispositif au regard de l'objectif poursuivi »[1943]. Aussi, le responsable de traitement doit se conformer au principe de minimisation des données qui doivent être adéquates et pertinentes. Le RGPD exige que seules les données nécessaires au traitement

---

[1939] RGPD, art; 6 §1 e) ; DPJ, art. 8 « le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1 » et art. 1 §1 : La DPJ concerne tout « traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ».

[1940] DPJ, art. 9 §1.

[1941] DPJ, art. 8 §2.

[1942] Compte tenu de l'incidence qu'engendrent les technologies de surveillance « augmentées » sur les droits et libertés, le traitement de DACP qu'elles opèrent doit au préalable faire l'objet d'une analyse d'impact sur la protection des données en application de l'article 27 de la DPJ et de l'article 35 du RGPD. Si le traitement est effectué par une autorité publique à des fins de prévention ou de répression des infractions alors l'analyse d'impact sur la protection des données devra être soumise à la consultation de la CNIL (LIL, art. 90).

[1943] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p.13.

soient collectées[1944] alors que la DPJ n'impose qu'une collecte non excessive des données[1945]. Toutefois, il convient de rappeler que le législateur a adopté des conditions d'exigence plus strictes à l'égard de la collecte des DACP par des drones aériens de sécurité publique[1946]. En toute logique, les DACP collectées par les algorithmes « augmentés » de sécurité publique associés aux drones aériens ne devraient traiter que les données de ces drones et *de facto* que les données strictement nécessaires au traitement. D'une manière plus générale, il conviendrait d'appliquer des règles similaires de minimisation du traitement des DACP à tous les dispositifs de surveillance « augmentés » de sécurité publique.

665. Garanties techniques des SIA de sécurité publique - Aussi, le traitement de DACP ne devra pas porter une atteinte disproportionnée aux droits et aux libertés. À cette fin, le responsable de traitement doit mettre en œuvre des garanties juridiques et techniques suffisantes (v. **n° 722-724 ; 796 et suiv.**). Les mécanismes permettant de manière effective d'assurer la protection de la vie privée et des DACP par défaut ou par conception[1947] doivent être adoptés afin de réduire les potentialités d'atteintes aux droits et libertés des personnes concernées. La CNIL considère plusieurs mesures qui pourraient apporter des garanties à la protection des DACP en matière d'algorithmes d'aide au traitement des images telles que sur « la qualité des images (abaissement de la définition, floutage, etc.), le nombre d'images traitées […], l'intégration de mécanismes permettant la suppression quasi immédiate des images sources ou la production d'informations anonymes »[1948]. La proportionnalité du recours aux technologies de surveillance « augmentées » de sécurité publique doit reposer sur une analyse détaillée de leur incidence sur les personnes concernées, des traitements de données envisagés (volume et type de données y compris les éventuelles données sensibles), des conditions de mise en œuvre (délimitation du périmètre et de la durée du recours au dispositif) ainsi que des garanties prévues afin de protéger les DACP (ex. anonymisation, accès aux seules personnes habilitées, etc.).

[1944] RGPD, art. 5 §1 c).

[1945] DPJ, art. 4 §1 c).

[1946] CSI, art. L. 242-4.

[1947] RGPD, art. 25 et DPJ, art. 20

[1948] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p.13.

666. Information des personnes du recours à des SIA de sécurité publique - Enfin, il convient de s'intéresser au devoir d'informer les personnes[1949] concernées par le traitement afin de respecter le principe de loyauté imposé par le RGPD et la DPJ[1950]. Si, toutefois, il peut être envisagé pour des raisons légitimes de limiter l'information des personnes[1951], le principe impose d'informer en des termes clairs et précis les personnes de l'existence d'un traitement impliquant leurs DACP[1952]. Néanmoins, la mise en œuvre de cette obligation dans la cadre du recours à des technologies de surveillance « augmentées » de sécurité publique s'avère particulièrement complexe puisqu'elle devra s'adapter au caractère novateur et « invisible »[1953] résultant de l'immatérialité de celles-ci. En ce sens, la CNIL estimait dans son étude sur les caméras « augmentées » qu' « une simple mise à jour des panneaux d'affichage d'un système de vidéoprotection […] ne saurait suffire » et encourageait les autorités publiques à fournir des informations sur des supports adaptés tels que des panneaux d'information plus spécifiques, des marquages au sol ou encore des annonces sonores[1954]. Dès lors, il s'avère essentiel de mettre en œuvre différentes mesures afin de porter à la connaissance du public l'existence d'un traitement par des caméras « augmentées » en appliquant un principe de transparence de leur emploi ainsi que d'explicabilité quant à leurs finalités et à leur mode de fonctionnement (v. **n° 750 et suiv.**). Aussi, d'autres mesures que celles regardant la protection des DACP devraient être mises en œuvre afin de renforcer les garanties protégeant les droits et libertés.

b. Les règles et principes généraux communs à mettre en œuvre pour encadrer les technologies de surveillance « augmentées » de sécurité publique

667. Les différents enjeux, précédemment exposés, concernant le développement et le recours à des technologies de surveillance « augmentées » de sécurité publique ne pouvant être entièrement résolus au moyen des dispositions relatives à la protection des DACP incitent à l'adoption de

---

[1949] RGPD, art. 12 à 15 et DPJ, art. 13 §§ 1 et 2.

[1950] RGPD, art. 5 §1 a) et DPJ, art. 4 §1 a).

[1951] DPJ, art. 13 §3.

[1952] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 45.

[1953] Ce caractère « d'invisibilité » technologique s'additionne à celui déjà constaté sur les drones aériens. Cet état de fait laisse place à une forme de surveillance davantage dissimulée en dépit des dispositions adoptées par le législateur.

[1954] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p.14.

mesures techniques et juridiques adaptées[1955]. Ces mesures prennent la forme de dispositions spécifiques aux SIA qu'expose le REIA[1956] ainsi que la future convention sur les SIA qu'adoptera le Conseil de l'Europe[1957]. Ces dispositions spécifiques reposent sur des règles et principes généraux communs des SIA dont certains ont déjà été formulés tels que la protection des droits de l'Homme et des libertés fondamentales ou encore le principe de transparence des traitements automatisés de données.

668. L'adoption du REIA suscite le débat de certains acteurs (principalement des concepteurs), qui s'opposent notamment à certaines règles interdisant la conception et l'usage de SIA, au motif qu'il pourrait conduire à freiner l'innovation[1958]. Aujourd'hui encore, la LIL fait elle aussi parfois l'objet de critiques ; certains lui reprochant son caractère trop contraignant[1959]. Pourtant, ce texte ne s'oppose pas à la collecte de DACP et, à l'inverse, autorise leur traitement de manière encadrée. Dès lors, les arguments des opposants à la mise en œuvre d'un cadre juridique général des SIA « résistent […] relativement mal à l'épreuve des faits, et les besoins d'une telle régulation se révèlent au-delà du simple constat de l'enchevêtrement des cadres juridiques potentiellement applicables »[1960]. À l'inverse, l'absence d'encadrement clair et correctement défini de la conception et de l'usage des SIA fait défaut. En ce sens et de manière concrète, cette absence de dispositions contraignantes à l'égard des SIA n'empêche ni leur développement ni leur recours mais constitue un péril pour les droits et libertés. À titre d'exemple, l'absence de dispositions spécifiques permettant d'encadrer le recours à des drones aériens équipés de caméras n'avait pas

---

[1955] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 74 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 243.

[1956] L'adoption du texte du REIA consacre ainsi le premier cadre juridique européen en matière d'IA compte tenu de la densité et de la richesse des propositions qu'il comporte.

[1957] La future convention-cadre pour l'IA (en cours d'élaboration par le Conseil de l'Europe) constituera un des premiers cadre juridique des SIA au monde qui, de surcroît, pourrait bénéficier à un plus grand nombre d'États que le REIA en ce qu'il ne se limite pas aux seules États membres de l'UE (à l'instar de la Convention 108+ sur la protection des DACP).

[1958] MUELLER (B.), "The Artificial Intelligence Act Is a Threat to Europe's Digital Economy and Will Hamstring The EU's Technology Sector In The Global Marketplace", *Center for Data Innovation*, April 21st 2021 [en ligne] ; CIMINO (V.), « Le futur règlement européen sur l'intelligence artificielle peut-il être un frein à l'innovation ? », *Siècle Digital*, 18 novembre 2021 [en ligne] consultés le 20 novembre 2020. L'amendement adopté par le Parlement européen le 14 juin 2023 suscite des critiques de la part d'industriels qui estiment que « la version de 2021 était plus équilibrée tandis que celle de 2023 en interdisant davantage de SIA, y compris uniquement à des fins de développement, constitue un frein à l'innovation » (Propos tenus par un membre d'IDEMIA lors du Webinaire « Loi "Jeux Olympiques" et biais algorithmiques » organisé le 22 juin 2023).

[1959] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 50.

[1960] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 326.

empêché - dans un premier temps - leur utilisation par les forces de l'ordre durant les confinements de l'année 2020 en France.

669. Aussi, l'absence d'encadrement des technologies de surveillance « augmentées » de sécurité publique ne permet pas de résoudre les enjeux qu'elles soulèvent notamment en matière de transparence de leur usage. La conception et l'utilisation sans encadrement approprié de ces technologies renforcent le climat de méfiance entre les personnes concernées, d'une part, et les concepteurs et utilisateurs, d'autre part. Dès lors, seul un encadrement juridique de la conception, des pratiques et du rôle des différents acteurs de la « chaine de vie » des technologies de surveillance « augmentées » de sécurité publique peut permettre d'écarter les recours abusifs ou illégaux à ces technologies. En outre, cet encadrement permettra de mettre en œuvre des mesures de lutte contre les menaces informatiques ou encore les discriminations que sont susceptibles d'amplifier les SIA. Dès lors, le REIA permet d'apporter des réponses aux inadéquations législatives subsistantes en matière d'encadrement des SIA principalement au moyen de deux procédés. D'une part, le REIA procède à leur classification en fonction du niveau de risque qu'ils engendrent, sans pour autant encadrer de manière spécifique chaque typologie de SIA en fonction du secteur d'activité dans lequel ils seront utilisés (i). D'autre part, le texte impose le respect de plusieurs règles et principes généraux communs aux SIA (ii).

i. La classification des SIA : une approche par les risques

670. Aux fins de lutter contre les atteintes qu'engendrerait une société de surveillance sur les droits et libertés, les institutions européennes préconisent l'élaboration d'un cadre juridique fondé sur une approche par les risques[1961]. Le REIA met en œuvre des mesures de classification des SIA selon quatre catégories en fonction du niveau de risque qu'ils présentent pour les droits et libertés : « interdits », « à hauts risques », « à risques limités » et « à risque minimes »[1962]. Le texte adopte

[1961] Dans son Livre blanc sur l'IA, la Commission européenne proposait déjà de mettre en place un cadre réglementaire européen de l'IA adoptant une approche fondée sur les risques (Commission européenne, « Livre blanc Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance », *op. cit.*, p. 12). Dans le même sens, le Conseil de l'Europe confirme vouloir adopter une approche similaire : « Le CAHAI [Comité *Ad Hoc* sur l'Intelligence artificielle] recommande qu'un futur cadre juridique du Conseil de l'Europe sur l'IA poursuive une approche basée sur les risques ciblant le contexte d'application spécifique » (CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 15) et « Lors de la mise en œuvre de mesures visant à prévenir les dommages, les États membres devraient adopter une approche fondée sur les risques » (*Idem*, pp. 30-31).

[1962] REIA, art. 3.

des lignes rouges interdisant l'usage de certains SIA[1963]. Ces interdictions répondent globalement aux attentes formulées par plusieurs institutions[1964] telles que l'EDPB et le CEPD, le Conseil de l'Europe ou encore la Commission nationale consultative des droits de l'homme (CNCDH) et le Sénat. Dès lors, les technologies de surveillance « augmentées » de sécurité publique ne pourront être utilisées à des fins de notation sociale, de catégorisation des individus en fonction de critères discriminants (ex. origine ethnique, sexe, orientation politique ou sexuelle ou autre motif condamné par le Code pénal[1965]) ou encore à de reconnaissance biométrique pour déduire les émotions d'une personne physique.

671. L'amendement du REIA adopté par le Parlement européen le 14 juin 2023 a modifié la liste des SIA interdits[1966] et ceux reconnus comme étant à « haut risque ». L'amendement du REIA est venu étoffer la liste des SIA devant être interdites. Elles concernent les SIA considérés comme intrusifs et discriminants tels que ceux à des fins policières incluant notamment l'identification biométrique à distance dans les espaces accessibles au public en temps réel[1967] et *a posteriori*[1968]. Cette mention explicite d'interdiction des technologies de surveillance biométriques au sein de l'espace public constitue une avancée majeure de telle sorte qu'elle dépasse l'unique interdiction de l'usage de technologies de reconnaissance faciale sur la voie publique. En ce sens, les députés répondent de manière concrète aux inquiétudes formulées par les organisations de défense des droits et libertés à l'inverse du législateur français et du Conseil constitutionnel qui ne faisaient

---

[1963] REIA, art. 5 §1.

[1964] EDPB, Avis conjoint 05/2021 de l'EDPB et du CEPD concernant la législation sur l'intelligence artificielle, *op. cit.*, pp. 12-14 ; Conseil de l'Europe - Comité consultatif de la Convention pour la protection des données des personnes à l'égard du traitement des données à caractère personnel (Convention 108), Lignes directrices sur « L'intelligence artificielle et la protection des données », 25 janvier 2019 [en ligne] ; CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, spéc. p. 15 ; CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, *op. cit.*, pp. 9-15 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., pp. 74-77.

[1965] CP, art. 225-1.

[1966] Pour rappel, les SIA présentant un niveau de risque inacceptable pour les droits et libertés des personnes sont strictement interdits et listés dans le REIA.

[1967] Amendement REIA, art. 5(1e) rec. (18), p. 131 : « The use of [AI systems for 'real-time' remote biometric identification of natural persons] in publicly accessible places should therefore be prohibited ».

[1968] Le texte introduit une exception à l'usage de SIA d'analyse biométrique d'images prises sur la voie publique soumise à une double condition dans le cadre de l'application de la loi à des fins de poursuites de crimes graves et uniquement sur autorisation de l'autorité judiciaire : « AI systems used for the analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems should also be prohibited, unless there is pre-judicial authorisation for use in the context of law enforcement, when strictly necessary for the targeted search connected to a specific serious criminal offense that already took place, and only subject to a pre-judicial authorization » [Amendement REIA, art. 5(1e) rec. (18), p. 131].

jusqu'ici mention que d'une interdiction des technologies de reconnaissance faciale[1969]. L'interdiction explicite de ces usages par les membres du Parlement européen permet de renforcer les garanties en matière d'usage des SIA par les forces de l'ordre. Elle se prolonge par une interdiction de recourir à des SIA ayant pour finalité la reconnaissance des émotions ou encore de police « prédictive »[1970]. En outre, la liste inclut l'interdiction de recourir à des SIA effectuant une catégorisation biométrique[1971].

672. Ces nouvelles interdictions s'accordent avec les recommandations formulées par la CNCDH, qui soulignait le haut potentiel d'atteintes aux droits et libertés pouvant remettre en question le maintien de l'anonymat dans l'espace public[1972]. La CNCDH avait, elle aussi, admis des exceptions lorsque ces usages étaient strictement nécessaires par exemple à « la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes » ou encore à la sécurisation des « ouvrages, installations et établissements d'importance vitale »[1973]. Dans le même sens, les sénateurs avaient approuvé l'adoption d'une interdiction de principe de ces usages et la possibilité d'autoriser « à titre très exceptionnel leurs recours par les forces de sécurité intérieure en cas de menace grave ou pour les besoins d'une enquête judiciaire sur une infraction grave »[1974]. Ils avaient notamment insisté sur le caractère impératif d'interdire le recours à ces usages lors de manifestations sur la voie publique ou à proximité des lieux de culte[1975]. Dès lors, l'interdiction formelle issue de l'amendement du REIA s'avère plus protectrice des droits et libertés mais ne

---

[1969] Voir en ce sens les garanties prévues par la loi RPSI en matière de protection des DACP dans le cadre de l'utilisation de caméras aéroportées (C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.* ; CSI, art. 242-4, al. 2). À l'exception de la loi JOP2024 portant sur l'expérimentation de caméras « augmentées » mais dont l'application dans ce domaine prendra fin au 31 mars 2025. Pour rappel, la reconnaissance faciale est une donnée biométrique mais il en existe bien d'autres telles que les empreintes digitales ou encore l'iris. La mention du terme de « données biométriques » permet d'inclure un plus grand nombre de techniques intrusives (puisqu'il s'agit de données sensibles) pouvant être utilisées à des fins de reconnaissance d'un individu et permet de palier les éventuels flous juridiques quant à leur traitement notamment par des algorithmes d'analyse d'images.

[1970] Amendement REIA, art. 5(1a) rec. (26a), p. 127 : Les SIA de police « prédictive » inclus le profilage, l'analyse des antécédents criminels, la géolocalisation .

[1971] Amendement REIA, art. 5(1a) rec. (16a), p. 127.

[1972] CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, *op. cit.*, p. 12

[1973] *Ibid*.

[1974] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 76.

[1975] *Idem*, p. 77.

permet aucune forme d'expérimentation telle que le souhaiteraient les autorités publiques[1976].

673. Indépendamment des interdictions que formule le REIA, celui-ci comprend une catégorie de SIA dits « à haut risque » dont il prévoit l'entièreté du régime juridique. Les SIA à l'usage des autorités publiques entrent principalement dans cette catégorie[1977]. Dès lors, le REIA crée plusieurs obligations relatives à la conception des SIA à l'égard des autorités publiques qui ont recours à des SIA qu'elles ont conçues. En revanche, le texte leur permet de bénéficier davantage de garanties lorsqu'elles ont recours à des SIA conçus par des tiers[1978]. Néanmoins, les États membres resteront libres dans le choix des normes (loi ou règlement) à adopter pour encadrer le recours spécifique à certains SIA. Ce choix pourrait s'effectuer selon que le SIA appartient ou non à la catégorie « à haut risque » à l'image des technologies d'analyse automatisée d'images captées dans l'espace public par des dispositifs fixes ou embarqués permettant la détection de situations anormales, d'infractions ou de menaces, sans même qu'il soit procédé à l'identification des personnes physiques[1979]. Après avoir catégorisé les SIA, les textes européens formulent plusieurs principes généraux afin de répondre aux enjeux que posent spécifiquement ces SIA.

ii. Les principes généraux communs applicables aux SIA

674. Le REIA, au même titre que la Convention-cadre sur l'IA, repose sur l'application de plusieurs principes généraux qui s'adapteront à tout type de SIA. Au sein de ces principes, le respect des droits de l'Homme et des libertés fondamentales constitue une priorité[1980]. À ce titre, le Conseil de l'Europe rappelait que « les instruments généraux […] de protection des droits de l'homme, notamment la Conv.EDH, la déclaration universelle des droits de l'Homme et la Charte des droits

---

[1976] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 46-47.

[1977] Les SIA « à haut risque » sont énumérés dans l'Annexe III du REIA qui recouvre essentiellement les activités régaliennes telles que la police et la justice.

[1978] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 136.

[1979] REIA, Annexe III. Voir sur ce sujet : CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 137.

[1980] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 30 : À ce titre, le CAHAI rappelle que « la prévention des dommages est un principe fondamental qui doit être respecté, tant dans la dimension individuelle que collective, en particulier lorsque ces dommages concernent l'impact négatif sur les droits de l'homme, la démocratie et l'État de droit ». De manière similaire, l'importance que revêt la protection des droits et libertés fondamentaux se retrouve dans tout le corps du REIA.

fondamentaux de l'Union européenne, s'appliquent à tous les domaines de la vie, y compris en ligne et hors ligne quelle que soit la technologie utilisée et donc également aux systèmes d'IA »[1981]. Le respect de ces droits et libertés permet aussi d'inclure la protection de la vie privée et des DACP ainsi que le principe de non-discrimination[1982].

675. Aussi, d'autres principes permettent de renforcer les garanties quant au recours à des technologies de surveillance « augmentées » de sécurité publique. En premier lieu, le principe de subsidiarité[1983] du recours aux technologies de surveillance « augmentées » de sécurité publique permettrait de s'assurer que les technologies disposent d'un haut niveau de fiabilité[1984] (v. **n° 709 et suiv.**) et ne peuvent être remplacées par des moyens moins intrusifs en vertu du principe de nécessité et de proportionnalité. À cette fin, le REIA exige un haut niveau de robustesse, de sécurité et d'exactitude ainsi que de qualité des jeux de données utilisées en vue d'entrainer les SIA. En deuxième lieu, le principe de transparence et les mesures en faveur de l'explicabilité des algorithmes[1985] (v. **n° 750 et suiv.**) permettent de lutter contre l'opacité qui entoure les technologies de surveillance « augmentées » de sécurité publique. Ils consistent à assurer la compréhension du fonctionnement du SIA, principalement par les utilisateurs mais aussi par les personnes concernées, ainsi que l'information de ces dernières s'agissant du traitement de leurs DACP par des technologies de surveillance « augmentées » de sécurité publique. En dernier lieu, le texte encourage le recours à des solutions technologiques souveraines[1986] (v. **n° 765 et suiv.**) qui permettent d'assurer une plus grande protection des droits et libertés des personnes (respect des

---

[1981] *Idem*, p. 20.

[1982] *Idem*, pp. 33-34 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 113-118.

[1983] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 77.

[1984] REIA, art. 15 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 108-112 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 43.

[1985] REIA, art. 13 ; CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, pp. 34-36 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 118-125 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 78 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 49.

[1986] REIA, art. 10 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 43 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 130-134 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., pp. 102-107.

droits des personnes sur les données d'apprentissage lorsqu'elles incluent des DACP et mesures de sécurisation des données traitées par le SIA).

676. En outre, le REIA introduit des exigences relatives aux mesures d'ordre technique reposant sur des moyens à mettre en œuvre en vue d'assurer aux autorités publiques une maitrise de leurs technologies. Ces exigences concernent les mesures techniques (et juridiques) en matière de cybersécurité[1987] (v. **n° 786 et suiv.**) et celles instaurant un principe de primauté humaine[1988] qui inclut notamment le contrôle humain[1989] sur le SIA (v. **n° 780 et suiv.**). Aussi, les rédacteurs du REIA ont introduit des sanctions en cas de non-respect des règles relatives aux SIA classés comme étant à « risque élevé » ou interdits (« risques inacceptables »). De manière assez cohérente, le texte prévoit des sanctions similaires à celles du RGPD et de la DPJ qui pourront prendre la forme d'amendes administratives dont le montant (plus sévère) peut s'élever à trente millions d'euros ou 6% du chiffre d'affaires[1990].

677. Néanmoins, il convient de préciser que le REIA n'a pas vocation à imposer toutes les normes qui devront régir les SIA en France. À l'inverse d'autres actes d'encadrement comme la DPJ, la Commission européenne a, cette fois, pris la décision « de proposer un unique instrument juridique, sous la forme d'un règlement d'effet direct »[1991] aux fins d'encadrer les SIA, y compris ceux qui seront utilisés par les forces de l'ordre. Face à ce choix, le Conseil d'État faisait remarquer, dans son étude sur les SIA publics, que l'encadrement de ces derniers, compte tenu de la spécificité de leurs finalités de puissance publique, auraient pu bénéficier d'un encadrement supranational plus

---

[1987] REIA, art. 15 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 43-44 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 126-127.

[1988] Ce principe repose sur « l'idée qu'un humain doit veiller à ce que les systèmes d'IA fonctionnent à son bénéfice, se porter garant de leur bon fonctionnement et répondre aux conséquences de ses dysfonctionnements » (CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 98).

[1989] REIA, art. 14 (exigence réitérée dans le Compromis d'amendement de la Proposition de REIA du Parlement européen du 11 mai 2023 (art. 4 a) p. 143) ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 77 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 102-106 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 44.

[1990] REIA, art. 71.

[1991] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 136.

souple[1992]. Néanmoins, la position adoptée par les institutions européennes d'élaborer un règlement et non une directive (plus communément adoptée en vue d'encadrer de nouveaux domaines) s'est imposée dans un souci d'assurer l'uniformité et l'applicabilité directe des règles mises en œuvre[1993]. Dès lors, sans même attendre l'adoption du REIA et de la Convention-cadre sur l'IA, les États membres doivent adopter des dispositions ou des lignes directrices afin d'appliquer une méthodologie et des conditions permettant le développement et le recours à des technologies de surveillance « augmentées » de sécurité publique.

2. L'adoption de nouvelles normes juridiques nationales pour encadrer les différents cas d'usage des technologies de surveillance « augmentées » de sécurité publique

678. Dans une perspective d'amélioration de la sécurité publique, les autorités françaises ont prévu de recourir à des drones aériens « augmentés » afin d'assurer, notamment, la surveillance de grands évènements. Cependant, il n'existe aujourd'hui aucune disposition pérenne prévoyant l'usage de technologies de traitement d'images[1994]. Avant l'adoption de la loi JOP2024 autorisant - de manière expérimentale et temporaire - le recours à ces technologies, certains acteurs considéraient que dans la mesure où aucune donnée biométrique ne faisait l'objet d'un traitement, les technologies de traitement d'images pouvaient être utilisées dans le cadre juridique actuel[1995]. De fait, le recours à ces caméras « augmentées » n'est pas par principe illicite et le régime relatif à la vidéoprotection du CSI ne s'opposerait pas à leur utilisation[1996]. Néanmoins, la CNIL estime que ces technologies conduisent à des traitements de DACP de nature distincte à celle des caméras

---

[1992] *Ibid*. La question peut être posée de savoir s'il n'aurait pas fallu procéder de manière similaire s'agissant du cadre européen régissant la protection des DACP (RGPD et DPJ) en créant une directive, en parallèle du règlement, pour encadrer les SIA utilisés à des fins de police et de justice.

[1993] MARTI (G.), CLUZEL-MÉTAYER (L.) et MERABET (S.), « Droit et Intelligence artificielle », *JCP G* n° 26, 28 juin 2021, doctr. 720.

[1994] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 11 : « Aucune dispositions du CSI n'encadre, à ce jour, les conditions de mises en œuvre des dispositifs de vidéo « augmentées ».

[1995] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit*., p. 86 : « D'aucun considèrent que les techniques de traitement des images ne concernant pas des données biométriques permettant l'authentification ou l'identification des personnes peuvent être déployées à cadre législatif constant, dès lors que ces traitements s'inscrivent dans les mêmes finalités que celles attribuées aux systèmes de vidéoprotection ».

[1996] CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 11 : « En effet, le CSI n'a vocation à régir que les dispositifs relevant de son objet et n'empêche pas le déploiement d'autres dispositifs. En outre, pour les finalités qu'il régit, il n'encadre que la licéité de la captation d'image. […] Dès lors, selon la CNIL, le régime de la vidéoprotection prévu par le CSI, y compris ses dispositions pénales (art. L. 254-1), n'interdit pas toute utilisation de la vidéo "augmentée" ».

« non-augmentées » qui nécessitent dès lors des règles juridiques spécifiques encadrant les SIA. Celles-ci peuvent prendre la forme de lignes directrices générales qui s'adapteraient à tous les SIA (a) ou s'effectuer par une législation expérimentale qui traiterait les SIA au cas par cas (b).

a. La mise en œuvre de lignes directrices à l'usage des technologies « augmentées » destinées au secteur public

679. En l'absence de règles générales encadrant spécifiquement l'usage des SIA, le Conseil d'État recommande l'adoption de lignes directrices qui, à l'instar des chartes éthiques, permettraient de renforcer la confiance du public par la mise en œuvre de mesures adaptées aux différents usages des SIA et notamment à ceux destinés aux acteurs publics[1997]. À ce titre, il rappelle qu'en dépit de l'application du REIA, celui-ci ne dispense aucunement l'État du devoir d'adopter des mesures qui permettront de rendre effectifs les principes et les règles adoptées par les institutions européennes[1998]. Aussi, le Conseil d'État adopte une position en faveur des lignes directrices pour gérer les usages des SIA plutôt qu'une législation-cadre en admettant, toutefois, que cette forme pourrait convenir à l'encadrement spécifique de SIA publics. Néanmoins, l'adoption de lignes directrices peut constituer une première approche générale afin d'assurer la gestion du développement et des usages des drones aériens « augmentés » de sécurité publique.

680. Les lignes directrices pour les SIA permettent de définir la stratégie, la doctrine d'emploi ainsi que la méthodologie à adopter s'agissant tant de leur conception que de leur utilisation. En outre, elles rassembleraient l'ensemble des dispositions juridiques et des recommandations techniques pouvant déjà être appliquées aux SIA. Elles iraient dans le sens des propositions émises par la CNIL en 2017 qui encourageait les développeurs de SIA à adopter une position d'éthique dès la conception (*ethic by design*)[1999] afin de concevoir des algorithmes programmés pour respecter des principes éthiques. L'adoption de lignes directrices permet ainsi de mettre en application les pratiques juridiques et techniques assurant une première protection effective des droits et libertés. Face à la multiplication des usages en matière de caméras « augmentées », le recours à des lignes

[1997] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 138.

[1998] *Idem*, p. 139.

[1999] CNIL, « Comment permettre à l'Homme de garder la main ? - Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle », *op. cit.*, p. 41.

directrices constituerait une garantie supplémentaire au respect des droits et libertés.

681. Pour l'heure, les technologies de surveillance « augmentées » ont surtout fait leur apparition dans l'espace public par l'intermédiaire d'une phase d'expérimentation effectuée à droit constant. Cependant, plusieurs autorités ont souligné l'importance de mettre en œuvre un texte législatif ou réglementaire qui autoriserait ou encadrerait spécifiquement l'emploi de ces technologies au cas par cas[2000]. De fait, une expérimentation à droit constant implique que les règles juridiques en vigueur soient respectées (ex. consentement des personnes quant à l'utilisation de dispositifs de reconnaissance faciale sur la voie publique). Or, certaines expérimentations ne peuvent se faire à droit constant et nécessitent par conséquent l'adoption d'un texte spécifique.

b. L'adoption de dispositions juridiques expérimentales à l'usage des technologies de surveillance « augmentées » de sécurité publique

682. Les avis et recommandations du Conseil d'État et de la CNIL ont fait apparaitre un besoin de mettre en œuvre des dispositions juridiques adaptées aux usages des technologies de surveillance « augmentées » de sécurité publique[2001]. En ce sens, le Conseil d'État considère que les traitements d'images opérés par des SIA sont des traitements de DACP distincts de ceux issus de la vidéoprotection[2002]. À ce titre, il avait estimé que « compte tenu du changement d'échelle qu'ils impliquent dans la capacité d'exploitation des images de surveillance de la voie publique, [ces technologies] sont susceptibles de porter une atteinte […] à la liberté individuelle »[2003]. Dès lors, il

---

[2000] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, spéc. pp. 79-82 ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, pp. 15-16 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), op. cit., pp. 46-47.

[2001] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 137 : « L'analyse automatisée d'images captées dans l'espace public par des dispositifs fixes ou embarqués permettant la détection de situations anormales, d'infractions ou de menaces, sans même qu'il soit procédé à l'identification de personnes physiques […] sont susceptibles d'avoir des incidences plus ou moins importantes sur les libertés publiques selon l'usage auquel ils sont destinés ». Dès lors, leur développement « plaide, par précaution, pour qu'il soit inséré dans la loi de 1978 un régime-cadre suffisamment souple pour englober l'ensemble des SIA recourant à ce procédé technique, de préférence à une autorisation législative au cas par cas » ; CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 14 ; CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, *op. cit.* ; CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, *op. cit.*

[2002] CE, Avis du 12 octobre 2021, non publié : « les traitements des images issues de la vidéoprotection par le biais d'un logiciel d'intelligence artificielle constituent des traitements de données personnelles distincts de ceux des images issues de la vidéoprotection ».

[2003] *Ibid*.

avait formulé le besoin de mettre en œuvre une base législative explicite afin d'encadrer le recours à des SIA d'analyse d'images issues de caméras de vidéoprotection, y compris dans le cas où celles-ci ne traiteraient pas des données biométriques[2004]. D'une manière générale, concernant les technologies de surveillance « augmentées » de sécurité publique, le Conseil d'État se présente en faveur d'un régime reposant sur « les dispositions propres aux traitements ne nécessitant pas l'identification »[2005].

683. Dans le même sens, la CNIL avait estimé concernant les caméras « augmentées » de sécurité publique que compte tenu de leurs potentialités d'atteintes aux droits et libertés, leur mise en œuvre relevait du domaine de la loi au sens de l'article 34 de la Constitution[2006]. En ce sens, elle estimait que l'utilisation de ces technologies par les forces de l'ordre, même de manière temporaire et limitée à certains évènements, modifiait les effets de l'action des forces de l'ordre sur l'exercice des droits et libertés et que, dès lors, leur fondement juridique dépassait celui de la règlementation sur la protection des DACP[2007]. Ainsi, la CNIL affirmait que le recours à des caméras « augmentées » de sécurité publique pouvait porter atteinte aux droits des personnes s'étendant de la sphère pénale (liberté individuelle) aux conditions d'exercice de toutes les libertés individuelles et collectives (ex. liberté d'aller et venir, droit de manifestation, etc.)[2008]. Aussi, face aux enjeux que suscite le recours aux caméras « augmentées » de sécurité publique, il est recommandé au législateur d'adopter un cadre expérimental pour les caméras « augmentées » de sécurité publique afin de ne pas pérenniser trop rapidement des usages qui ne sont pour l'heure pas encore bien maitrisés et dont les conséquences ne sont peut-être pas encore toutes connues[2009].

2004 *Ibid*.

2005 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 137.

2006 CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », *op. cit.*, p. 15.

2007 *Ibid* : Ainsi, la CNIL affirmait que « les traitements algorithmiques de détection des comportements "suspects" ou infractionnels emportent un changement de degré et de nature dans la surveillance à distance de la voie publique que le législateur a souhaité encadrer il y a plusieurs années au sein du CSI pour les caméras de vidéoprotection "classiques" ».

2008 *Idem*, pp. 15-16.

2009 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, spéc. pp. 46-47 ; Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, spéc. pp. 79-82.

684. L'expérimentation est plébiscitée pour encadrer les technologies « augmentées » de sécurité publique[2010] dans la mesure où elle permet de déterminer si celles-ci répondent aux finalités de nécessité et de proportionnalité exigées en matière de mesures de police et de s'assurer que les niveaux de compétence, de contrôle ainsi que de conformité correspondent aux attentes[2011]. Aussi, ce procédé permet de « repenser le besoin au regard de la balance coût/avantages, sans céder à la course en avant que semble faire naitre la masse de données à analyser, compte tenu d'un recours de plus en plus fréquent à la vidéoprotection »[2012]. D'une manière générale, l'expérimentation permet de déterminer le cadre juridique qui serait le plus adapté à l'usage de ces technologies.

685. Suivant la volonté des défenseurs des droits et libertés, la loi JOP2024 vient encadrer l'expérimentation des caméras de vidéoprotection « augmentées » en autorisant leur recours de manière limitée dans le temps et dans l'espace à des fins de surveillance des grands évènements se déroulant en 2023 et 2024[2013]. Cependant, il convient d'insister sur le fait que le terme d' « expérimentation » ne doit pas seulement être envisagé comme une simple limitation des usages dans le temps mais comme une phase de test[2014]. Les conclusions du rapport d'analyse de l'expérimentation des caméras « augmentées » de sécurité publique conduite sous la loi JOP2024 permettront de déterminer si l'usage de cette technologie par les forces de sécurité publique permet effectivement de remplir les exigences tant en matière de garanties des droits et libertés, d'une part, qu'en matière de résultats opérationnels attendus, d'autre part. De fait, ces expérimentations doivent faire l'objet d'une évaluation à l'issue de la période préalablement établie par le texte. Il serait alors tout à fait envisageable que, dans le cas où les évaluateurs présenteraient un bilan positif de ces

---

[2010] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 79 : « Cette phase d'expérimentation semble faire consensus ». Le projet de loi déposé par le Sénat, le 12 juin 2023, portant sur les usages de systèmes de reconnaissance biométrique au sein de l'espace public (Sénat, Proposition de loi n° 128 relative à la reconnaissance biométrique dans l'espace public, 12 juin 2023 [en ligne]) tend a confirmé cette attrait pour les lois d'expérimentation de ces technologies. L'adoption de ce texte autoriserait l'expérimentation des technologies de reconnaissance faciale dans des cas d'usage exceptionnels justifiés par un intérêt public supérieur soumis à des autorisations préalables et une procédure de contrôle permanent.

[2011] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 46. L'expérimentation repose sur une méthode en trois temps : expérimentation, évaluation et potentielle pérennisation.

[2012] Sénat, Rapport d'information n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 79.

[2013] Néanmoins, il est regrettable que ces expérimentations se déroulent pendant les grands évènements et non pas en amont tel que formulé dans le Rapport de Jean-Michel Mis (préc. cité., p. 47).

[2014] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 38 : « Les expérimentations sont souvent perçues comme une première étape, sans possibilité réelle de retour en arrière (« effet cliquet »), et non comme un moyen de vérifier la maitrise de la technologie, son cadre d'emploi et de contrôle et les améliorations à apporter pour un éventuel usage à l'avenir ».

expérimentations, le recours à des caméras de vidéoprotection « augmentées » puisse être pérennisé par un nouveau texte législatif adapté étendant son champ d'application temporel et spatial. De fait, d'autres technologies mises en œuvre de manière expérimentale ont par la suite été intégrées de manière définitive dans la législation. Il en est allé ainsi du recours aux caméras individuelles (*bodycams*) telles que celles portées par les agents des forces de l'ordre[2015] ou ceux des services de secours[2016]. Dès lors, le législateur devra se montrer vigilant lorsqu'il prendra la décision de pérenniser des mesures « provisoires » (mesures d'exception) venant restreindre l'exercice des droits et libertés[2017].

686. Les évolutions technologiques fulgurantes ont inévitablement induit un retard de la législation permettant leur encadrement. Ce constat mérite d'être pris en considération par le législateur lorsqu'il élabore un texte en la matière[2018]. En ce sens, le texte de la LIL fait office de référence dans la mesure où la définition de son champ d'application a permis d'y introduire d'autres formes de technologies qui n'existaient pas lors de sa publication en 1978. Dès lors, le législateur doit adopter une vision à plus long terme et anticiper les évolutions technologiques afin que la loi puisse encadrer les pratiques futures. En d'autres termes, le législateur doit concevoir une nouvelle approche de la conception des lois portant sur les nouvelles technologies. Aussi, au vu des conséquences que peuvent avoir les technologies de surveillance « augmentées » de sécurité publique, la législation doit envisager des moyens juridiques concrets permettant d'assurer aux

---

[2015] La loi n° 2016-731 du 3 juin 2016, *op. cit.*, avait introduit dans un premier temps la possibilité pour les agents de la police municipale de procéder à des enregistrements audiovisuels de leurs interventions au moyen de caméras individuelles de manière expérimentale. Les résultats relevés par le rapport d'évaluation de l'expérimentation des caméras mobiles par la police municipale avaient permis de dresser un bilan très favorable à la pérennisation de leur utilisation (Ministère de l'Intérieur, Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale, 7 juin 2018 [en ligne]). La loi n°2018-697 du 3 août 2018 (relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique, *JORF* n°0179 du 5 août 2018, [en ligne]) a permis d'introduire de manière définitive dans le CSI l'utilisation de caméras individuelles par les agents de la police municipale.

[2016] La loi du 3 août 2018 (préc.) était venue étendre le champ d'application de l'utilisation des caméras mobiles individuelles aux agents des services de secours à titre expérimental. Cette utilisation fut également pérennisée par la loi n° 2021-1520 du 25 novembre 2021 (visant à consolider notre modèle de sécurité civile et valoriser le volontariat des sapeurs-pompiers et les sapeurs-pompiers professionnels, *JORF* n°0275 du 26 novembre 2021 [en ligne]), art. 57 désormais codifié à l'article L.241-3 du CSI.

[2017] Depuis une dizaine d'années, une tendance visant à inscrire de manière durable dans le droit commun des dispositions relevant du régime d'exception semble progressivement s'installer. À l'image de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *op. cit.*, venant pérenniser les dispositions de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *op. cit.*, qui comprenait pourtant des mesures relevant du régime de l'état d'urgence suite aux attentats qui avaient eu lieu en France. Voir notamment : SAFI (F.), « La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement - Entre pérennisation et extension de l'exception », *op. cit.*

[2018] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 22.

personnes concernées la possibilité d'agir en réparation d'un préjudice qu'elles auraient subi conséquemment de l'usage de cette technologie.

B. Le droit au recours juridictionnel, support de la protection des droits et libertés face aux technologies de surveillance « augmentées » de sécurité publique

687. Les technologies de surveillance « augmentées » de sécurité publique, ayant vocation à participer à la prise de décision dans le cadre des missions de prévention et de répression des atteintes à l'ordre public, nécessitent la mise en œuvre du droit au recours juridictionnel effectif. De fait, il s'avère essentiel que les personnes susceptibles de faire l'objet d'une décision reposant partiellement sur les résultats d'un SIA ayant une incidence négative sur leurs droits et libertés puissent contester la décision lorsqu'elles s'estiment lésées. L'utilisation de SIA par les autorités publiques doit dès lors s'accompagner de la mise en œuvre du droit au recours contre la décision ; en d'autres termes de la possibilité de contester la décision adoptée sur base des résultats du SIA, d'une part (1), et sur « la réparation des préjudices qu'ils ont causés, et, le cas échéant, sur l'engagement de la responsabilité pénale »[2019], d'autre part (2).

1. Les voies de recours juridictionnel opposables aux technologies de surveillance « augmentées » de sécurité publique

688. Le Conseil d'État est le premier à avoir affirmé le droit au recours juridictionnel effectif lors d'un arrêt d'assemblée du 17 février 1950[2020] lui attribuant la valeur de principe général du droit. Il est aujourd'hui reconnu comme une liberté fondamentale de la procédure de référé-liberté par le juge administratif[2021]. Le Conseil constitutionnel a également reconnu le droit au recours juridictionnel[2022] et lui a conféré le statut de droit de valeur constitutionnelle[2023] en se fondant sur

---

[2019] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 144.

[2020] CE, ass., 17 février 1950, n° 86949, *Dame Lamotte* [en ligne] : En l'espèce, le juge administratif avait autorisé le recours pour excès de pouvoir contre tout acte administratif y compris en l'absence de texte l'autorisant.

[2021] CE, ord., 13 mars 2006, n° 291138, *Bayrou et Association de défense des usagers des autoroutes publiques de France* [en ligne].

[2022] C. const., Décision n° 93-335 DC, 21 janvier 1994, *Loi portant diverses dispositions en matière d'urbanisme et de construction*, Rec. p. 40 [en ligne].

[2023] C. const., Décision n° 96-373 DC, 9 avril 1996, *Loi organique portant statut d'autonomie de la Polynésie française*, Rec. p. 43 [en ligne].

l'article 16 de la DDHC[2024]. Au niveau européen, le droit au recours juridictionnel effectif s'est vu attribuer le statut de principe général du droit de l'Union par la CJUE[2025] avant d'être finalement inscrit dans la CDFUE[2026]. Ce droit est également affirmé par le droit européen[2027] et se trouve indirectement lié au droit à un procès équitable[2028] qui confère la possibilité à chaque personne d'accéder à une justice indépendante et impartiale[2029]. La CEDH a donné une interprétation étendue au droit au recours juridictionnel dans le sens où la violation du droit protégé par la Convention ne doit pas être avérée mais seulement que l'allégation de son atteinte soit « plausible » et « défendable »[2030].

689. Aussi, pour la CEDH le droit au recours juridictionnel est lié au droit à un procès équitable, reconnu comme étant un droit fondamental[2031], ayant vocation à garantir une égalité entre les parties devant le juge et à conserver l'effectivité du débat contradictoire au procès civil comme au procès pénal[2032]. Or, le principe du contradictoire suppose que les parties au procès puissent avoir connaissance et débattre de toutes les pièces ou observations présentées au juge[2033]. Ce droit obligerait les autorités publiques faisant usage d'une technologie de surveillance « augmentées » de communiquer des éléments permettant d'expliquer le résultat produit par le SIA nécessitant par conséquent une maitrise du fonctionnement de cette technologie par les différents acteurs y compris par les magistrats. Dans le cadre de l'utilisation de drones aériens « augmenté » de sécurité

2024 DDHC, art. 16 : « Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution ».

2025 CJCE, 15 mai 1986, *Marguerite Johnston*, aff. C-222/84 [en ligne]. Voir aussi : CJUE, 22 décembre 2010, *DEB mbH c. Allemagne*, aff. C-279/09 [en ligne].

2026 CDFUE, art. 47 §§ 1 et 2 : « Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal » et « a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi ».

2027 ConvEDH, art. 13 : « Toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officiels ».

2028 Conv.EDH, art. 6 §1 : « toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle ».

2029 CEDH, gd. ch., 21 février 1975, *Golder c. Royaume-Uni*, n° 4451/70 [en ligne] ; CEDH, 26 février 2002, *Fretté c. France*, n° 36515/97 [en ligne].

2030 CEDH, 27 avril 1988, *Boyle et Rice c. Royaume-Uni*, n° 9659/82 [en ligne].

2031 SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, p. 94.

2032 CEDH, 17 janvier 1970, *Delcourt c. Belgique*, n° 2689/65 [en ligne].

2033 CEDH, gd. ch., 20 novembre 1989, *Kostovski c. Pays-Bas*, n° 11454/85 [en ligne] ; CEDH, 27 mars 1998, *J.J c. Pays-Bas*, n° 21351/93 [en ligne] ; C. const., Décision n° 2015-713 DC, 23 juillet 2015, *Loi relative au renseignement*, *op. cit.*

publique, l'obstacle d'un recours juridictionnel pourrait se situer dans l'absence ou l'insuffisance de mesures permettant aux personnes concernées d'avoir connaissance de l'analyse effectuée par un SIA[2034] ou de maitriser ses finalités par manque d'explicabilité. En ce sens, le Conseil d'État soulignait les difficultés pouvant être rencontrées en vue de contester la légalité d'un traitement de données qui n'avait fait l'objet d'aucun décret ou arrêté, à l'exception d'une saisine de la CNIL lorsque le traitement porte sur des DACP[2035]. Les drones aériens dont les forces de l'ordre avaient fait usage durant les confinements entrent précisément dans ce cas de figure[2036] et leur utilisation avait donné lieu à une demande en référé-liberté auprès du juge administratif par la *Quadrature du Net* conséquemment à l'absence de demande d'avis à la CNIL et du dépôt de l'analyse d'impact sur la protection des données.

690. Le juge administratif pourrait déjà être saisi concernant des cas de traitements algorithmiques impliquant des DACP[2037] au moyen du recours pour excès de pouvoir contre un acte règlementaire, qui permet de contrôler la légalité d'un acte administratif[2038]. En ce sens, le juge administratif a eu l'occasion de statuer, dans le cadre d'un recours pour excès de pouvoir, concernant un traitement de DACP ayant eu lieu sans qu'aucun texte règlementaire n'ait imposé sa création[2039]. De même, il serait possible d'agir devant le Conseil d'État par la voie du référé-liberté[2040], en cas d'atteinte grave et manifestement illégale à une liberté fondamentale par une technologie de surveillance « augmentée » de sécurité publique en vue de demander en urgence l'arrêt ou la modification du recours au SIA d'aide à la prise de décision (ou SAAD)[2041]. Dès lors, une personne qui se considérerait lésée par une décision prise sur le fondement des résultats d'une

---

2034 L'obligation d'information en matière de traitement de DACP par un SIA s'avère particulièrement complexe à mettre en œuvre lorsque le traitement est effectué à partir d'un drone aérien.

2035 CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 145.

2036 Voir en ce sens : CE, ord., 18 mai 2020, n°440442, *op. cit.* ; CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155, *op. cit.* ; CNIL, Délibération n°SAN-2021-003, *op. cit.*

2037 Notamment dans le cadre d'un traitement de DACP effectué en application des articles 31 ou 32 de la LIL.

2038 GAUDEMET (Y.), *Droit administratif*, *op. cit.*, p. 159.

2039 CE, , 2ème - 7ème ch., 6 novembre 2019, *Fédération des acteurs de la solidarité et autres*, n° 434376 [en ligne] et n° 434377 [en ligne].

2040 CJA, art. L. 521-2.

2041 CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 145.

technologie de surveillance « augmentée » de sécurité publique pourrait se voir reconnaitre un droit de présenter sa cause devant un juge.

691. Cependant, le pouvoir d'intervention du Conseil d'État est limité, dans la mesure où il revient aux autorités publiques de prendre la décision de faire usage d'un SIA et seul un usage explicitement interdit (tel que la reconnaissance faciale s'agissant des drones aériens) pourrait lui permettre d'agir. En outre, les SIA posent d'importantes difficultés d'ordre technique aux juges qui ne pourront effectuer un contrôle de la légalité de leur utilisation ou des décisions prises sur leur fondement par les forces de l'ordre que dans la mesure où ils disposeront d'une maitrise suffisante de leur fonctionnement[2042].

2. L'application du principe de responsabilité aux technologies de surveillance « augmentées » de sécurité publique

692. Les autorités publiques et, le cas échéant, les concepteurs qui déploient des technologies de surveillance « augmentées » de sécurité publique doivent endosser la responsabilité du fait de leurs résultats sur les décisions prises à l'encontre des personnes concernées[2043]. Ces acteurs devraient pouvoir être tenus par une obligation de rendre des comptes (*accountability*) lorsque les normes juridiques reposant sur des principes généraux communs ne sont pas respectées ou qu'une personne a subi un préjudice[2044]. Aussi, l'élaboration d'un régime de responsabilité du fait de ces technologies devrait pouvoir concilier les intérêts des personnes ayant souffert d'un préjudice résultant pour part d'un SIA et ceux des concepteurs et utilisateurs[2045].

693. La notion de responsabilité suppose que toute personne doit répondre de ses actes devant la justice lorsqu'ils ont causé un dommage à autrui et d'en assumer les conséquences (civiles,

---

[2042] *Idem*, p. 147.

[2043] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 38 ; REIA, cons. 58 : « Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux potentiellement associés à leur utilisation […] il convient de définir des responsabilités spécifiques pour les utilisateurs ». Voir aussi : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 388-389.

[2044] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 38.

[2045] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 148.

pénales administratives)[2046]. Cependant, le recours à des technologies de surveillance « augmentées » de sécurité publique peut générer des difficultés quant à l'identification de l'origine de la décision dommageable prise à l'encontre d'un individu et de la détermination du responsable ainsi que du lien de causalité. Ces difficultés résultent principalement de la multiplicité des acteurs impliqués et de l'opacité subsistante de certains SIA qui complexifie la « traçabilité des erreurs »[2047].

694. Le fait dommageable peut résulter d'un dysfonctionnement de la technologie de surveillance « augmentée » de sécurité publique (défaut de conception ou de développement opposable au concepteur), d'un défaut d'utilisation ou d'interprétation des résultats de l'algorithme d'analyse d'images par l'agent ayant pris la décision finale, ou encore d'un tiers malveillant dont l'attaque porterait soit sur la caméra (atteinte à l'intégrité des données collectées) soit sur le SIA (atteinte aux résultats de l'algorithme d'analyse d'images). Dans ce dernier cas, la personne ayant subi le dommage pourrait engager une procédure en responsabilité civile sans faute reposant sur un motif d'insuffisance de sécurisation de l'outil (imputable au concepteur) ou sur un motif d'imprudence de l'utilisation de l'outil ayant permis la cyberattaque[2048].

695. Il est possible d'envisager différents types de responsabilité selon la personne concernée et l'existence d'une faute (intentionnelle ou non-intentionnelle). Le recours à des technologies de surveillance « augmentées » par les forces de l'ordre serait susceptible de mettre en jeu leur responsabilité devant le juge administratif (a). Aussi, la responsabilité pénale, du concepteur ou de l'agent (utilisateur), pourrait être potentiellement engagée si une faute était avérée (b).

a. La responsabilité administrative du recours aux SIA par les forces de l'ordre

696. Le préjudice subi par un individu suite au recours à des technologies de surveillance « augmentées » par les forces de l'ordre est susceptible d'engager la responsabilité de la puissance

---

[2046] CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 821. Voir aussi : DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 150.

[2047] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 148.

[2048] *Idem*, p. 149.

publique. La décision du Tribunal des conflits dans l'arrêt *Blanco*[2049] consacre la responsabilité de l'État quant aux dommages causés par ses agents et la compétence de la juridiction administrative en la matière. Elle suppose l'obligation pour l'administration de réparer les dommages résultants des actions ou inactions des personnes physiques agissant pour le compte de l'État[2050]. Aussi, la question du partage de cette responsabilité entre l'administration et ses agents a été résolue par la décision *Pelletier*[2051] où le Tribunal des conflits a introduit la distinction entre la responsabilité de service[2052] et la responsabilité pour faute personnelle[2053].

697. Il serait possible d'engager la responsabilité pour faute afin d'obtenir la réparation du préjudice causé par un acte administratif, en l'occurrence un acte de police, effectué sur le fondement des résultats produits par un SAAD. La faute de l'administration pourrait toujours être engagée si la décision est illégale[2054] telle qu'une décision prise sur le fondement d'une technologie utilisée illégalement (ex. absence d'autorisation) ou à des fins interdites (ex : traitement de données biométriques par une caméras « augmentée » filmant la voie publique en l'absence d'un cadre légal adapté). De même, le résultat erroné d'un SIA ayant conduit à une décision illégale engagerait la responsabilité de l'administration. En ce sens, le Conseil d'État estime que l'administration ne peut s'exonérer de sa responsabilité au motif que les SAAD auxquels elle a recours sont déficients[2055]. La mise en œuvre de la responsabilité administrative suppose que la personne ayant subi le

---

[2049] TC, 8 février 1873, *Blanco*, *op. cit.* : « Considérant que la responsabilité, qui peut incomber à l'État, pour les dommages causés aux particuliers par le fait des personnes qu'il emploie dans le service public, ne peut être régie par les principes qui sont établis dans le Code civil » et « que cette responsabilité n'est ni générale, ni absolue ; qu'elle a ses règles spéciales qui varient suivant les besoins du service et la nécessité de concilier les droits de l'État avec les droits privés » alors « l'autorité administrative est seule compétente pour en connaître ».

[2050] DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 564.

[2051] TC, 30 juillet 1873, *Pelletier*, *op. cit.*

[2052] La faute de service est celle qui est rattachée à l'exercice des fonctions de l'agent ou des agents agissant pour le compte de l'État. Elle peut résulter d'un agent identifiable (faute de service individuelle) ou être anonyme engageant le service dans son ensemble (faute du service public). Voir notamment : CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, pp. 403-404 ; GAUDEMET (Y.), *Droit administratif*, *op. cit.*, p. 197.

[2053] À l'inverse, la faute personnelle est l'acte dommageable commis par un agent agissant pour le compte de l'État en dehors de ses fonctions ou dans le cadre de ses fonctions mais qui, manifestement, ne répond pas au comportement susceptible d'être attendu par l'administration de la part de ses agents (faute intentionnelle ou faute grave). Voir notamment : CORNU (G.) (dir.), *Vocabulaire juridique*, *op. cit.*, p. 404 ; DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 584.

[2054] GAUDEMET (Y.), *Droit administratif*, *op. cit.*, p. 197 ; PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 726.

[2055] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 150.

préjudice démontre un lien de causalité entre la faute commise et le dommage[2056]. Cependant, il peut s'avérer complexe d'établir tant l'existence d'une faute que le lien entre celle-ci et le dommage subi.

698. Le juge pourrait également apprécier l'existence d'une faute de l'administration en procédant à l'examen des actes de celle-ci selon qu'elle ait recours à un SIA ou non. Dès lors, il serait possible de mettre en cause la responsabilité de l'administration lorsque celle-ci a manqué à une de ses obligations en tant qu'utilisatrice d'un SIA[2057]. Le juge pourrait apprécier l'existence d'un manquement de l'administration en se référant aux exigences prévues par le REIA en matière de sécurité et de contrôle humain des SIA[2058]. En ce sens, l'administration est tenue par un devoir de vigilance à l'égard de l'utilisation des SIA.

699. La responsabilité de l'administration peut également être engagée en l'absence de faute dans le cas où une personne aurait subi un grave préjudice conséquemment à l'utilisation d'un SIA. Le Conseil d'État a effectivement reconnu très tôt la possibilité d'engager la responsabilité de l'État pour les agissements de l'administration même non fautifs[2059]. Cette responsabilité a pour conséquence de décharger la victime d'un préjudice de la démonstration de l'existence d'une faute de l'administration afin d'être dédommagée[2060]. Cette responsabilité pourrait être engagée sur plusieurs fondements dont celui d'une rupture d'égalité des administrés devant les charges publiques. La responsabilité sans faute de l'administration s'avère ainsi particulièrement adaptée dans le cadre du recours à des technologies de surveillance « augmentées » de sécurité publique et plus généralement des SIA.

700. Enfin, il convient de mentionner le fait que le REIA ne comprend aucune disposition spécifiquement dédiée à la responsabilité du fait des SIA. Dès lors, il revient aux États membres et à leurs juridictions de « définir le niveau de risque socialement acceptable en contrepartie des

---

[2056] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 734 ; DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 605.

[2057] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 150.

[2058] REIA, art. 14 et 15.

[2059] CE, 21 juin 1895, *Cames*, Rec. p. 509.

[2060] DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, *op. cit.*, p. 621.

bénéfices attendus de la mise en service de ces systèmes »[2061]. Aussi, deux principes pourraient être mis en œuvre dans le cadre de l'indemnisation du préjudice subi par les victimes d'une décision d'une technologie de surveillance « augmentée » de sécurité publique. En premier lieu, la complexité d'un SIA ne doit pas permettre à l'administration de pouvoir se décharger de sa responsabilité. En deuxième lieu, l'action en responsabilité engagée par les victimes des dommages du fait d'un SIA ne devrait concerner que l'administration. En d'autres termes, il ne revient pas aux personnes ayant subi un préjudice d'engager la responsabilité d'autres acteurs tels que les concepteurs du SIA. En ce sens, l'administration devra s'assurer que les clauses contractuelles établies avec les fournisseurs de leurs SIA prennent dûment en compte les différents enjeux possibles pouvant engager la responsabilité de ces derniers envers elle.

701. Indépendamment de la responsabilité administrative pouvant être engagée du fait des SIA publics, il est également intéressant de réfléchir à la possibilité de mettre en jeu la responsabilité pénale conséquemment à l'usage de cette technologie.

b. La mise en œuvre de la responsabilité pénale du fait des SIA

702. Au préalable, il convient d'exclure toute possibilité d'envisager une quelconque responsabilité du SIA comme étant un sujet de droit autonome[2062]. Certains auteurs et institutions européennes[2063] s'étaient posés la question de savoir s'il était envisageable de doter les SIA d'une personnalité juridique permettant aux personnes de mettre en cause leur responsabilité[2064]. Cette solution se révèle inadaptée au regard des régimes de responsabilité en vigueur[2065] et dans la mesure

---

[2061] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 152.

[2062] Voir en ce sens : CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 149 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 151 ; JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 81 ; MESA (R.), « Intelligence artificielle et droit pénal : quels responsables, quelles infractions, quelles responsabilités ? », *RLDI* n° 181, mai 2021, pp. 34-39, spéc. p. 35.

[2063] Parlement européen, Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique 2015/2103 (INL) [en ligne] ; BENSOUSSAN (A.), « Plaidoyer pour un droit des robots : la "personne morale" à la "personne robot" », *La Lettre des juristes d'affaires*, 23 octobre 2013, n° 1134.

[2064] Au motif que certains SIA délivrent des résultats sur base d'un fondement inexplicable, y compris par leurs concepteurs, il avait été imaginé de leur attribuer une personnalité juridique ainsi qu'un patrimoine propre aux fins de leur faire endosser la responsabilité lorsque des dommages étaient engendrés.

[2065] Voir notamment sur ce sujet : Cour d'appel de Paris, Rapport du groupe de travail sur « La réforme du droit français de la responsabilité civile et les relations économiques », avril 2019, 109 p., spéc. pp. 107-109 [en ligne].

où elle repose essentiellement sur une recherche d'exonération de la responsabilité des concepteurs (et possiblement des utilisateurs). De fait, la responsabilité pénale d'un SIA ne peut être engagée puisqu'elle ne se conçoit qu'à l'égard des personnes physiques[2066]. Ces technologies ne sont que des outils conçus par des êtres humains qui doivent en endosser la responsabilité selon le principe de primauté humaine qui suppose qu'un humain s'assure que le SIA fonctionne et réponde aux finalités exigées[2067]. Dès lors, la responsabilité du fait des technologies de surveillance « augmentées » de sécurité publique revient à une personne physique ou morale impliquée dans leur conception ou leur utilisation.

703. Aussi, s'il ne peut être imputé une quelconque forme de responsabilité pénale à une machine, les règles relatives à la responsabilité du fait de l'infraction commise par un animal pourraient trouver à s'appliquer[2068]. De fait, le droit pénal reconnait la responsabilité qui pèse sur le propriétaire ou le gardien de l'animal lorsque ce dernier a commis une infraction[2069]. En d'autres termes, la personne qui a le contrôle de l'animal au moment des faits endosse la responsabilité pénale de ses actes[2070]. De même, le droit pénal a déjà été confronté à des formes d'IA lorsque les premiers véhicules autonomes ont été mis en circulation et que leurs premières infractions sont apparues[2071]. Les réflexions sur le sujet offrent dès lors plusieurs pistes pour envisager la responsabilité pénale du fait des technologies de surveillance « augmentées » de sécurité publique. L'infraction pénale serait ainsi imputable à la personne sous le contrôle de laquelle se trouvait le SIA, conformément à l'article 121-1 du CP, qui peut être soit son concepteur soit son utilisateur. La détermination de la personne responsable devrait donc être effectuée au cas par cas. Elle pourrait notamment reposer sur la part du contrôle décisionnel laissée à l'usager par le SIA. Ainsi, la responsabilité pénale du concepteur devrait être la responsabilité de principe lorsqu'il s'agit d'un

---

2066 CP, art. 121-1 et 121-2.

2067 CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 98. Voir aussi : CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 31.

2068 C. civ., art. 515-14.

2069 C. cass., ch. crim., 19 février 1957, Bull. crim. n° 165 ; C. cass., ch. crim., 3 juin 1957, Bull. crim. n° 466.

2070 C. cass., ch. crim., 29 mai 2013, n° 12-85.427 [en ligne] ; C. cass., ch. crim., 21 janvier 2014, n° 13-80.267 [en ligne].

2071 Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite « Loi Pacte », art. 125 [en ligne]. Voir notamment sur ce sujet : Dossier « Le procès de l'intelligence artificielle et de la voiture autonome », *Dalloz IP/IT* n° 11, 16 novembre 2018, p. 578 et suiv. ; BÉNÉJAT-GUERLIN (M.), « Le droit pénal de la route face aux nouveaux modes de transports », *AJP* n° 9, 25 septembre 2019, p. 428.

SIA autonome[2072]. Cette responsabilité s'avère toutefois plus complexe à déterminer s'agissant des SAAD.

704. Les technologies de surveillance « augmentées » de sécurité publique relèvent des systèmes d'aide à la prise de décision. Dès lors, les erreurs de ces SIA, qui engendreraient un préjudice à une personne concernée par leurs traitements, seraient susceptibles d'engager la responsabilité pénale du concepteur comme celle d'un agent des forces de l'ordre. La responsabilité d'un agent pourrait notamment être engagée s'il a effectué une modification du SIA ou encore s'il a fait preuve d'imprudence ou de négligence dans son utilisation qui ont conduit à l'erreur de ce dernier. Dès lors, la détermination de la personne responsable relèvera de l'appréciation des juges. Outre l'identification de la personne responsable du préjudice, l'élément intentionnel sera également complexe à qualifier dans la mesure où les erreurs du SIA peuvent ne pas être constitutives d'une faute[2073].

705. Le droit pénal qualifie les dommages qui ne relèvent pas d'une faute d'infractions non intentionnelles. L'élément moral qualificatif d'une infraction non intentionnelle peut notamment se caractériser par l'imprudence, la négligence ou encore le manquement à des obligations légales de sécurité de son auteur[2074]. Dès lors, un agent pourrait être tenu pour responsable pénalement de l'erreur commise par le SIA s'il peut être démontré qu'il a « soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité »[2075] qu'il ne pouvait ignorer. Le juge aura donc le devoir d'apprécier le respect des exigences attendues du concepteur ou de l'agent utilisateur et de déterminer une limite à partir de laquelle le manquement peut être considéré comme excusable ou non. Aussi, l'élaboration de normes européennes harmonisées fixant les standards de fiabilité des SIA de même que les procédures de certification devraient contribuer à la mission du juge dans son appréciation de l'existence ou non

---

[2072] MESA (R.), « Intelligence artificielle et droit pénal : quels responsables, quelles infractions, quelles responsabilités ? », *op. cit.*, spéc. p. 36.

[2073] CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 44.

[2074] CP, art. 121-3 §3.

[2075] CP, art. 121-3 §4.

d'un manquement[2076]. En outre, le juge pourrait également évaluer l'existence d'un manquement au moyen d'une comparaison des performances pour une même tâche entre l'agent et le SIA.

706. D'une manière générale, s'il est envisageable pour une personne ayant subi un préjudice du fait d'un SIA d'engager la responsabilité pénale du concepteur ou de l'agent, il est en revanche certain que des manquements délibérés, tels qu'un usage de SIA interdits ou encore d'un SIA haut risque illégalement[2077], engagerait des sanctions pénales. Enfin, il conviendra d'envisager de nouvelles règles européennes en matière de sanction pénale à l'encontre des concepteurs comme des utilisateurs de SIA. À ce sujet, le REIA renvoie au régime de sanctions des États membres de l'UE.

707. La mise en œuvre de règles aux fins d'encadrer le développement et l'usage des SIA constitue une première garantie du respect des droits et libertés face au recours à des technologies de surveillance « augmentées » de sécurité publique. Toutefois, le caractère effectif de cette garantie suppose que les concepteurs et utilisateurs mettent en œuvre des mesures de contrôle suffisantes, d'une part, et que les autorités chargées d'assurer le contrôle de ces technologies bénéficient des moyens nécessaires aux besoins requis par leurs nouvelles fonctions, d'autre part.

§2. Un renforcement des mesures de contrôle dès la conception des technologies de surveillance « augmentées » de sécurité publique

708. La garantie d'assurer une protection effective des droits et libertés repose sur la mise en œuvre de plusieurs mesures de contrôle dès la conception des technologies de surveillance « augmentées » de sécurité publique. La prévention des atteintes aux droits et libertés consiste notamment pour les concepteurs à satisfaire aux exigences de fiabilité, de sûreté[2078] et de cybersécurité (v. **n°405-412**)[2079]. Ces moyens préventifs doivent être complétés par des mesures

[2076] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 154.

[2077] En d'autres termes, qui ne rempliraient pas les obligations prévues par le REIA en matière de SIA à haut risque.

[2078] Ici, le terme de sûreté fait référence à la sûreté individuelle à laquelle pourrait porter atteinte un algorithme contenant des erreurs ou des biais dont les résultats mèneraient à une arrestation voire une condamnation arbitraire d'un individu.

[2079] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 31.

d'évaluation préalable et post-expérimentale de ces technologies[2080] (A). Aussi, il convient de renforcer les mesures de contrôle existantes en matière de recours aux technologies de sécurité publique afin d'intégrer les nouveaux enjeux que suscitent leur association à des SIA (B).

A. La mise en œuvre de moyens pour renforcer la fiabilité et l'efficacité des technologies « augmentées » de sécurité publique

709. Dans l'objectif d'assurer un certain contrôle des technologies de surveillance « augmentées » de sécurité publique, le REIA introduit des obligations à l'égard des concepteurs de mettre en œuvre des mesures permettant d'assurer l'exactitude et la robustesse des SIA[2081]. Ces mesures ont pour objectif de garantir la fiabilité des résultats présentés par le SIA. À cette fin, plusieurs recommandations et propositions de solutions ont été proposées en vue d'assurer un niveau de performance, de fiabilité, d'équité et de non-discrimination des SIA (1). Aussi, le contrôle de la conception et des usages de ces technologies nécessite la mise en œuvre d'une évaluation par les différents acteurs tout au long du cycle de vie des SIA (2).

1. Les mesures envisageables pour assurer la performance et lutter contre les biais algorithmiques

710. L'élaboration de dispositions juridiques pour encadrer les technologies de surveillance « augmentées » de sécurité publique est essentielle mais ne peut suffire pour garantir de manière effective la protection des droits et libertés. Dès lors, le recours à ces technologies nécessite la mise en œuvre de mesures techniques préalables par les concepteurs en vue de remplir un certain niveau de performance[2082] (ou d'efficacité) minimum et ne pas réduire le niveau de qualité attendu des services publics[2083] (a). Aussi, il a été démontré dans la première partie que les algorithmes étaient susceptibles de reproduire les biais (volontaires et involontaires) de leurs concepteurs qui

---

[2080] *Ibid* : « Les systèmes d'IA doivent être dûment testés et vérifiés avant leur utilisation ainsi que tout au long de leur cycle de vie, notamment par des examens périodiques visant à réduire ces risques au minimum ».

[2081] REIA, art. 15.

[2082] Laboratoire national de métrologie et d'essais (LNE), « Référentiel de certification de processus pour l'IA », 2021 [en ligne] : La performance peut être définie comme le « degré selon lequel un système ou composant accomplit ses fonctions désignées avec un ensemble de contraintes données, telles que la vitesse, la précision ou l'utilisation de la mémoire... ».

[2083] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 108.

conduisent à des décisions discriminatoires (v. n° **384 et suiv.**). Aujourd'hui, les chercheurs disposent de plusieurs pistes prometteuses en vue de limiter les biais algorithmiques (b).

a. La conception de SIA performants et fiables pour assurer la sécurité publique

711. En vue d'assurer un niveau de fiabilité et d'efficacité adéquat, la conception des SIA doit reposer sur trois étapes comprenant différentes exigences : une description des attentes des utilisateurs d'un SIA (objectifs), l'élaboration du SIA, et une procédure de validation du SIA[2084]. Lors de la première étape, qui consiste en l'élaboration d'un cahier des charges, les forces de l'ordre et les services de secours travaillent avec les concepteurs[2085] afin de définir les objectifs attendus du SIA qui équipera le drone aérien de sécurité publique. La deuxième étape est la plus complexe en ce qu'elle nécessite de remplir plusieurs exigences relatives notamment au choix de l'algorithme et au choix des données d'apprentissage. Enfin, la troisième étape repose sur des phases de tests du SIA à l'aide d'échantillons de données d'entrainement permettant d'évaluer son niveau de performance.

712. Les facteurs de performance - Outre le choix de l'algorithme le plus adéquat pour répondre aux finalités demandées, la performance du SIA dépend principalement de la qualité et de la pertinence des données d'apprentissage[2086]. La vérification de la qualité et de la quantité des données d'apprentissage est essentielle dans la mesure où celles-ci peuvent être de sources différentes et ne pas être destinées à des fins d'apprentissage automatique[2087]. La composition des jeux de données d'apprentissage constitue souvent une difficulté pour les concepteurs qui ne disposent pas toujours de données légales et adéquates pour entrainer leurs algorithmes[2088]. Face à cette difficulté, le Sénat serait favorable à une facilitation de l'accès à des jeux de données aux

---

2084 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 207.

2085 Les concepteurs peuvent être des agents internes aux services des forces de l'ordre ou des services de secours travaillant avec les agents de terrain à la conception de l'algorithmes. Il peut aussi s'agir d'entreprises privées intervenant en tant que membres d'un consortium à l'élaboration de solutions technologiques dans le cadre d'un projet de recherche (ANR, FUI ou encore Horizon Europe).

2086 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 10 ; CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 112.

2087 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 210.

2088 Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 69.

organismes de recherche qui leur permettrait d'assurer un meilleur entrainement de leurs algorithmes[2089].

713. Le REIA exige que les jeux de données d'entraînement, de validation et de test soient pertinents, représentatifs, exempts d'erreurs et complets[2090]. Or, cette exigence semble peu réalisable voire impossible s'agissant de garantir l'algorithme contre toutes erreurs. De fait, cette technologie reposant sur des statistiques[2091], elle ne peut fournir des résultats parfaitement fiables ; tout au plus peut-elle proposer des résultats avec un haut niveau de fiabilité (au-delà de ce que pourrait accomplir un être humain). La solution adoptée par le REIA ne peut être qu'une exigence de moyen permettant de sanctionner le recours, de manière intentionnelle ou par négligence, de jeux de données comportant des erreurs manifestes. En outre, il s'avérera difficile de garantir le caractère complet des jeux de données qui pourrait d'ailleurs se confronter au principe de minimisation des données si celles-ci se révèlent inadaptées aux finalités de l'algorithme[2092].

714. Les critères de performance - Le niveau de performance du SIA dépend de plusieurs conditions que sont la robustesse technique, l'exactitude, le temps de réponse de l'algorithme ainsi que l'adéquation à la demande formulée par les utilisateurs des caméras de surveillance « augmentées » de sécurité publique. La robustesse du SIA est un élément crucial pour ces technologies dans la mesure où elle permet de neutraliser les anomalies (ex. la luminosité ou encore le contraste d'une image). Elle suppose d'assurer la disponibilité, le fonctionnement et l'intégrité du SIA notamment lorsqu'il est intégré dans un objet connecté tel que les drones aériens de sécurité publique.

715. L'exactitude du SIA s'inscrit dans la continuité des exigences issues de la règlementation relative à la protection des DACP et peut être défini comme « l'absence d'écart entre la prévision, la

---

2089 *Idem*, pp. 104-106.

2090 REIA, art. 10.

2091 MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 1 : « L'apprentissage automatique et ses dérivés ne sont, en effet, qu'une manière parmi d'autres de créer de l'information en donnant du sens à des données par diverses méthodes statistiques ».

2092 Conseil de l'Union européenne, Rapport n° 13802/1/21 sur l'état des travaux de la proposition de REIA (législation sur l'intelligence artificielle), 22 novembre 2021, p. 7 §25 [en ligne] : « L'exigence selon laquelle les jeux de données d'entraînement, de validation et de test devraient être exempts d'erreurs et complets semble pratiquement impossible à satisfaire dans la plupart des scénarios. […] si cela devait être le cas dans la mesure du possible, il ne devrait pas s'agir d'une exigence absolue ».

décision ou l'action de la machine et la "bonne réponse" »[2093], c'est à dire équivalente à celle d'un humain ou objectivement bonne. En d'autres termes, les SIA doivent être conçus de manière à produire le moins d'erreurs possibles (faux positifs ou faux négatifs). À cette fin, les concepteurs de SIA doivent déterminer les paramètres[2094] à privilégier selon les finalités prévues qui reposent sur la justesse (*accuracy*), la précision (*precision*) ou encore la sensibilité (*recall*) et peuvent être complémentaires. Il est possible d'optimiser le SIA de différentes manières afin qu'il réponde au mieux au contexte d'utilisation.

716. Le paramètre de précision semble particulièrement convenir aux technologies de surveillance « augmentées » de sécurité publique en matière de police administrative puisqu'il repose sur une évaluation des bonnes réponses positives (vrais positifs) sur le total de réponses positives. Il permet d'éliminer les faux positifs et ainsi d'éviter les fausses alertes aux forces de l'ordre[2095]. Aussi, compte tenu de la gravité que pourrait engendrer une erreur de l'algorithme sur la personne ayant commis une infraction (atteinte à la liberté individuelle des personnes), la priorité doit être d'éliminer les faux positifs. Le paramètre de sensibilité vise à calculer le pourcentage des prévisions positives (vrais et faux positifs) du SIA sur la totalité des réponses objectivement positives. Dès lors, il constitue un paramètre intéressant dans la mesure où il permettrait de réduire le nombre de faux négatifs et de s'adapter tant aux missions de recherche ciblée d'un individu par les forces de l'ordre qu'aux missions d'alertes incendies. Le paramétrage du SIA est donc une étape primordiale puisqu'elle permet de minimiser les erreurs et devrait être réalisée au travers d'une collaboration entre les juristes, les mathématiciens et les informaticiens en vue de garantir l'adéquation entre les paramètres choisis et le cadre juridique[2096].

717. Niveau de performance - Le niveau minimal de performance acceptable devra être défini, en fonction des finalités recherchées, par les concepteurs du SIA équipant les systèmes de vidéoprotection en accord avec les forces de l'ordre ou les services de secours qui en feront usage. La détermination du niveau adéquat dépend de plusieurs facteurs. En premier lieu, le niveau

---

[2093] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 109.

[2094] Le REIA les désigne sous le terme de « métriques » (art. 9 §7 et 15 §2) dérivé du terme anglo-saxon *metrics* et peuvent être aussi appelés « indicateurs »: ils sont en quelque sorte les critères à privilégier.

[2095] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 210.

[2096] PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

minimal de performance acceptable doit prendre en considération le niveau de gravité que présente la présence d'erreurs dans les décisions rendues. Plus les conséquences d'une décision erronée sont susceptibles d'engendrer une atteinte aux droits et libertés d'un individu plus le niveau de fiabilité de l'algorithme doit être élevé. Les SIA à hauts risques, tels que les technologies de surveillance « augmentées » de sécurité publique, requièrent ainsi un haut niveau de fiabilité dans la mesure où leurs erreurs sont susceptibles d'avoir de graves conséquences pour les personnes, notamment leur liberté individuelle. En deuxième lieu, le niveau de performance doit être nivelé selon qu'il s'agisse d'un SIA entièrement autonome ou d'un SAAD. De fait, la présence humaine, qui assure la décision finale, permet de pallier un éventuel niveau de performance insuffisant. Dès lors, l'exigence quant au niveau de performance minimal acceptable du SIA pourra être limité s'agissant des technologies de surveillance « augmentées » de sécurité publique, celles-ci n'ayant vocation qu'à assister les forces de l'ordre et les services de secours lors des missions. En troisième lieu, il convient de tenir compte de l'acceptabilité sociale de ces technologies notamment quant aux investissements financiers qu'elles engendrent[2097]. Il s'agirait de ne pas reproduire les écueils de la vidéoprotection fixe dont les résultats modérés et le niveau d'efficacité non-évalué a eu pour conséquence de ternir l'image de ce moyen de sécurité publique[2098]. Enfin, ces technologies devraient être adoptées dans un objectif de renforcement des activités de sécurité publique et non conduire à une régression de l'efficacité des services rendus par les prestations humaines des forces de l'ordre ou des services de secours.

718. Le principe de performance devra ainsi être arbitré avec celui d'explicabilité dans la mesure où ils entretiennent des liens dont les finalités peuvent s'opposer. En ce sens, l'élévation du niveau de performance tend à réduire l'explicabilité de l'algorithme et inversement[2099]. Aussi, si les mesures favorisant la performance des algorithmes se justifient pleinement dans une idée de maintien de l'effectivité des activités de sécurité publique, la conception de ceux-ci mériterait de

---

[2097] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.* : « Dans le contexte des menaces de sécurité qui pèsent sur notre pays, les termes d'un débat de qualité, favorisant l'émergence de l'acceptabilité sociale, ne sont jamais posés » (p. 12) et « Tous les problèmes de sécurité ne nécessitent pas une intervention de la même ampleur, un même investissement technologique, une même mobilisation humaine. Adopter une focale citoyenne, c'est concentrer les esprits autour d'un objectif, pour se donner la liberté d'innover et d'expérimenter sur les meilleurs moyens d'y parvenir » (p. 51).

[2098] Tel que démontré au début de la Première partie.

[2099] CE, Étude sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 112.

favoriser davantage les objectifs d'égalité et de non-discrimination ainsi que d'explicabilité[2100].

b. Vers une conception des SIA équitables et non-discriminants

719. Le recours à des technologies de surveillance « augmentées » de sécurité publique pourrait engendrer des atteintes au principe de non-discrimination ainsi qu'au droit à l'égalité de traitement des personnes filmées (v. n° **377 et suiv.**). De fait, plusieurs études ont démontré que les SIA étaient susceptibles de reproduire voire d'exacerber les biais discriminatoires ou préjudiciables et les inégalités[2101] engendrant de graves conséquences pour les personnes concernées par le traitement ainsi que sur la société en général[2102]. Or, les actions des forces de l'ordre sont soumises aux principes d'égalité et de non-discrimination. Dès lors, il convient d'adopter des choix d'équité et de corriger les biais auxquels peut être sujet l'algorithme.

720. L'équité du SIA - L'exigence du respect des principes d'égalité et de non-discrimination suppose que le SIA réponde à des critères d'équité. L'équité consiste, s'agissant des algorithmes, à intégrer des contraintes dans leur programme. Les travaux sur l'équité algorithmique remontent à 2008[2103] où des chercheurs avaient proposé une méthode permettant d'établir une « règle de classification dite éthique »[2104]. Par la suite, les recherches dans ce domaine se sont étendues à d'autres disciplines. Aujourd'hui, l'équité est reconnue comme étant un concept éthique mais aussi pluriel au regard de la justice entre les personnes[2105]. Parmi les multiples conceptions de l'équité se trouvent l'équité horizontale et l'équité verticale[2106]. La première consiste à traiter de manière égale toute personne quel que soit son origine ethnique, son âge ou son genre par exemple. À l'inverse, la

---

[2100] DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », *op. cit.*, p. 10.

[2101] EUBANKS (V.), *Automating inequalities. How High-tech tools profiles, police, and punish the Poor*, New-York, St. Martin's Press, 2018, 272 p. ; Conseil de l'Europe, « Discrimination, intelligence artificielle et décision algorithmiques », 2018, 99 p. [en ligne] ; BUOLAMWINI (J.) and GEBRU (T.), "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *PMLR* 81, 2018, pp. 1-15 [en ligne] ; PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *op. cit.*

[2102] CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 33.

[2103] PEDRESHI (D.) *et al.*, "Discrimination-aware Data Mining", International Conference on *Knowledge Discovery and Data Mining*, 2008, pp. 560-568 [en ligne].

[2104] BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 15.

[2105] KOLM (S. C.), *Justice and Equity*, MIT Press, 1998, 275 p.

[2106] BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 15.

deuxième suppose de traiter différemment des personnes lorsqu'il existe des inégalités entre-elles. Ainsi, l'équité horizontale pourrait plus facilement se prêter aux usages des caméras « augmentées » de sécurité publique.

721. L'équité peut donc être intégrée aux algorithmes et ce par différents moyens. Il existe notamment une méthode d'équité appelée « anti-classification » qui permettait à un algorithme de ne pas tenir compte des qualifications protégées (ex. origine ethnique, genre, religion, etc.) dans son analyse et de proposer un résultat identique pour tout individu indépendamment de son appartenance à un groupe[2107]. Ce modèle d'équité pourrait convenir aux technologies de surveillance « augmentées » de sécurité publique dans un cadre de police administrative notamment. Aussi, il convient de mentionner qu'il n'existe aucune règle universelle de conception des algorithmes d'équité permettant de prévenir toutes les formes de discrimination[2108] et que les règles d'équité sont incompatibles entre-elles[2109]. D'une manière générale, les concepteurs devront formaliser ces choix d'équité dans les paramètres du SIA. Aussi, ce choix de concevoir des algorithmes équitables se conjugue avec les exigences de non-discrimination qui incitent à mettre en œuvre des mesures contre les biais algorithmiques.

722. Les mesures pour limiter les biais algorithmiques - La présence de biais à l'origine de discriminations peut s'expliquer notamment par le fait qu'un algorithme ayant pour finalités l'analyse d'individus « est par nature discriminant au sens où il distingue, discerne et traite différemment les individus en fonction de certaines de leurs caractéristiques […] »[2110]. Dès lors, la limitation de potentielles formes de discriminations nécessite que le traitement des données par l'algorithme s'effectue à partir de critères objectifs et socialement acceptables. Face aux risques que présentent les biais des SIA pour les droits et libertés des personnes, les concepteurs doivent appliquer différentes mesures techniques aux algorithmes. Le *Big Data* a ouvert de nouvelles conceptions de la recherche en donnant l'accès à une quantité massive de données numérisées. Les

---

2107 CORBETT-DAVIES (S.) *et al.*, "The Measure and Mismeasure of Fairness: A Critical Review of Fair Machine Learning", *Journal of Machine Learning Research* 24, 2018 (revised in August 2023) [en ligne].

2108 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 16.

2109 FRIEDLER (S.) *et al.*, "On the (im)possibility of fairness", 2016 [en ligne] ; LOFTUS (J. R.) *et al.*, "Causal Reasoning for Algorithmic Fairness", June 6th 2018 [en ligne] ; BERK (R.) *et al.*, "Fairness in criminal justice risk assessments : The state of the art", June 26th 2018 [en ligne].

2110 BASDEVANT (A.) et MIGNARD (J-P.), *L'empire des données : Essai sur la société, les algorithmes et la loi*, *op. cit.*, p. 96.

données sont plus nombreuses mais présentent l'inconvénient de n'être ni classifiées ni de contenir des informations quant à leur provenance ce qui engendre des difficultés aux chercheurs pour corriger les biais. Néanmoins, plusieurs pistes ont été déployées. Les chercheurs peuvent entreprendre de compléter un jeu de données en reconstituant les données manquantes à l'aide d'un modèle statistique. Cependant, cette solution comprend des limites dans le cas où le modèle serait lui-même biaisé ou s'il manquait des variables essentielles[2111].

723. Une autre solution repose sur la théorie des sondages qui consiste au redressement de l'algorithme en introduisant des variables auxiliaires qui corrigent les biais de sélection[2112]. En d'autres termes, cette technique permet d'expliquer et de corriger l'exclusion de certains groupes d'individus du fait que l'algorithme n'a pas été entrainé sur des jeux de données représentatives de la population générale. Les variables auxiliaires servent donc à compléter l'information. Enfin, les SIA peuvent être confrontés à d'autres difficultés lorsqu'ils sont mis en œuvre à des fins d'analyse de données en temps réel telle que dans le cas des technologies de surveillance « augmentées » de sécurité publique. Les SIA soumis à des contraintes de temps très courts pour effectuer leurs analyses auraient tendance à ignorer certaines caractéristiques des événements observés. Ainsi, les chercheurs insistent sur l'importance que revêt l'introduction de modèles temporels comprenant des instructions sur les mécanismes d'évolution des évènements analysés dans les méthodes d'apprentissage du SIA[2113]. En outre, et d'une manière générale, la prévention des discriminations suppose que les agents qui ont recours à des SIA soient informés et formés à ces enjeux afin d'avoir conscience des atteintes que peuvent engendrer ces technologies sur les droits et libertés de chacun et en faire ainsi usage de manière proportionnée.

724. Il est donc possible de corriger les biais algorithmiques et de concevoir des SIA équitables en fonction des finalités prévues. Aussi, les exigences de contrôle des SIA dès la conception doivent inclure des évaluations de leur fonctionnement tout au long de la vie de l'algorithme.

[2111] FAN (J.), FANG (H.) and HAN (L.), "Challenges of Big Data Analysis", *National Science Review* 1(2), October 26, 2013, pp. 293-314 [en ligne].

[2112] BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 13-14.

[2113] *Idem*, p. 14.

2. Les mesures d'évaluation des technologies de surveillance « augmentées » de sécurité publique

725. La conception des SIA se termine par une phase de validation qui consiste pour les développeurs à vérifier que les systèmes répondent effectivement aux exigences requises. En d'autres termes, les concepteurs effectuent une première évaluation du SIA pour s'assurer qu'il remplit les conditions demandées. Dans son étude sur les aspects juridiques de l'IA, le Conseil des barreaux européens avait insisté en ce sens sur l'importance que revêtait l'évaluation des technologies basées sur l'IA « dès les premières étapes de leur développement afin de minimiser le risque d'incidence négative »[2114] sur les droits et libertés. Néanmoins, l'introduction des technologies de surveillance « augmentées » de sécurité publique ne peut se limiter à une validation en amont par les concepteurs pour remplir les critères d'acceptabilité sociétale. Dès lors, celles-ci requièrent davantage de garanties qui peuvent prendre la forme d'une évaluation technique et opérationnelle effectuée par les forces de l'ordre et les services de secours (a). Aussi, la mise en œuvre des principes généraux communs aux SIA peut être effectuée au travers de la réalisation d'une étude d'impact de ces technologies (b).

a. Évaluation et auditabilité des technologies de surveillance « augmentées » de sécurité publique

726. Les technologies de surveillance « augmentées » de sécurité publique, étant des SIA à haut risque, doivent faire l'objet d'un contrôle préalable par une évaluation de conformité[2115]. La mise en œuvre de mesures d'évaluation et d'audibilité est primordiale en matière d'usage de technologies par les forces de l'ordre et les services de secours dans la mesure où elle permet de garantir leur performance et de favoriser leur acceptabilité sociétale. Aussi, l'exécution d'une évaluation des technologies de surveillance « augmentées » de sécurité publique se justifie pleinement dans la mesure où il n'est possible de contrôler « que ce qu'on peut évaluer, sans quoi la loi ne peut être interprétée correctement, pire la justice perd son principe de transparence fondamentale pour un traitement équitable entre les individus »[2116]. Cependant, ces mesures de

---

[2114] Conseil des barreaux européens (CCBE), Considérations du CCBE sur « les aspects juridiques de l'intelligence artificielle », 2020, 42 p., p. 14 [en ligne].

[2115] REIA, art. 43.

[2116] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 23.

contrôle sont chronophages et nécessitent d'établir en amont les conditions de leur réalisation afin de ne pas entraver l'action des services de sécurité publique[2117].

727. Une évaluation préalable est effectuée par les concepteurs lors de la phase de validation du SIA afin notamment d'identifier les facteurs susceptibles d'engendrer des erreurs ou des biais. À cette fin, le REIA prévoit que les SIA classés à haut risque, tels que le seront les technologies de surveillance « augmentées » de sécurité publique, doivent être munis d'un document technique remis par les concepteurs[2118]. Cette évaluation constitue une première garantie de confiance à l'utilisation d'un SIA. Néanmoins, cette évaluation pourrait également être assurée de manière complémentaire par différents acteurs tiers. En ce sens, le mathématicien Cédric Villani recommandait d'accroitre l'audibilité des SIA[2119]. À cette fin, la CNIL se présente comme un atout de taille puisqu'elle est déjà compétente pour effectuer des audits dans le cadre des contrôles relatifs aux traitements de DACP[2120].

728. Des entités tierces indépendantes pourraient également assurer cette évaluation complémentaire par un audit ou une certification de la qualité du SIA. À cette fin, le LNE a travaillé à l'élaboration d'un référentiel de certification[2121]. Aussi, les travaux de normalisation de l'association française de normalisation (AFNOR) en matière d'IA pourraient servir de références à des fins de certification des SIA après une phase d'audit[2122]. De même, le REIA attribue une place importante à la normalisation et prévoit que les exigences auxquelles sont soumis les SIA à haut risque soient consignées dans des normes harmonisées[2123]. En ce sens, l'évaluation de conformité

2117 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 54.

2118 REIA, art. 11 : « La documentation technique relative à un système d'IA à haut risque est établie avant que ce système ne soit mis sur le marché ou mis en service et est tenu à jour » ; REIA, annexe IV : Ce document comprend des informations sur « les résultats imprévus prévisibles et les sources de risques pour la santé, la sécurité, les droits fondamentaux et la discrimination, compte tenu de la finalité prévue du système d'IA ».

2119 Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 21 : « Au-delà de la transparence, il est nécessaire d'accroître l'audibilité des systèmes d'IA. Cela pourrait passer par la constitution d'un corps d'experts publics assermentés, en mesure de procéder à des audits d'algorithmes, des bases de données et de procéder à des tests par tout moyens requis ».

2120 LIL, art. 8, I 2. h).

2121 Pour la certification des SIA : LNE, « Référentiel de certification de processus pour l'IA », *op. cit.*

2122 AFNOR, Normes IA « Grand Défi IA » [en ligne] qui recense les normes publiées ou en cours de publication relatives à l'IA.

2123 REIA, art. 40 ; Règlement UE n° 1025/2012 du 25 octobre 2012 relatif à la normalisation européenne, *JOUE*, n° L 316, 14 novembre 2012, art. 10 [en ligne].

des SIA[2124] devrait s'effectuer en recourant à ces normes harmonisées[2125]. Dès lors, compte tenu des enjeux que présentent les SIA à haut risque, l'obligation d'évaluation préalable pourrait être complétée par un contrôle préalable effectué par un organisme indépendant qui donnerait lieu, par exemple, à une certification[2126].

729. L'évaluation de la performance technique et opérationnelle des technologies employées par les forces de l'ordre et les services de secours peut s'effectuer au moyen d'expérimentations qui permettent de déterminer leur niveau d'efficacité et leur légitimité au regard des atteintes portées aux droits et libertés ainsi qu'aux coûts qu'elles engendrent[2127]. Pour rappel, ces expérimentations sont limitées dans l'espace et dans le temps et ces évaluations ont ainsi pour objectifs de déterminer si ces dispositifs assurent les conditions suffisantes en vue d'être pérennisés. Aussi, il est préconisé que les forces de l'ordre et les services de secours prennent en considération la prévention des risques du recours à des SIA notamment en matière de cybersécurité (v. **n°405-412**).

b. Les études d'impact des technologies de surveillance « augmentées » de sécurité publique

730. Le concept des études d'impact a été introduit par le RGPD et la DPJ qui prévoient la mise en œuvre préalable d'une analyse d'impact sur la protection des DACP de manière facultative voire obligatoire pour certains traitements portant sur des données qualifiées de sensibles[2128]. Sur un modèle similaire, la réalisation d'études d'impact des SIA est recommandée voire requise lorsque la technologie est susceptible d'engendrer des conséquences graves notamment sur les droits et libertés. D'une manière générale, une étude d'impact a pour objectif d'analyser l'incidence du recours à des SIA sur les personnes concernées par le traitement des DACP au regard des principes généraux communs et des exigences légales. Elle permet de déterminer si la technologie envisagée

---

[2124] REIA, art. 43.

[2125] REIA, art. 33 § 11. Voir aussi : HO-DAC (M.), « La normalisation, clé de voûte de la règlementation européenne de l'intelligence artificielle (*AI Act*) », op. cit.

[2126] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 55 : « Dans certains cas, les systèmes d'IA devront faire l'objet d'une évaluation des risques réalisée par un tiers indépendant, qui devra donc auditer leur fonctionnement ».

[2127] Pour les drones voir notamment : MOREL (J-F.) et ABELLARD (M.), « L'emploi des drones, de la gendarmerie au maintien de l'ordre », *op. cit.*, spéc. pp. 122-123.

[2128] RGPD, art. 35 et DPJ, art. 27.

serait socialement acceptable ou non en évaluant son adéquation aux principes concernés ainsi que son ratio bénéfices/risques[2129].

731. Il conviendrait que les propositions visant à mettre en œuvre des technologies de surveillance « augmentées » de sécurité publique fassent systématiquement l'objet d'une évaluation d'impact en amont ainsi que d'avis par le Conseil d'État et par les entités de contrôle telles que la CNIL. Le rapport parlementaire soumis par le député Jean-Michel Mis sur les technologies de sécurité soulevait ainsi que les propositions de loi n'étaient pas évaluées à la hauteur des enjeux notamment s'agissant d'introduire de nouvelles technologies à l'usage des forces de l'ordre[2130]. Il soulignait en ce sens que ces textes ne faisaient pas l'objet d'étude d'impact ni d'avis de la part des autorités de contrôle conséquences de l'absence de dispositions contraignantes[2131]. À l'inverse, les projets de loi sont soumis à plusieurs contraintes qui exigent la réalisation d'une étude d'impact remise systématiquement au Conseil d'État et éventuellement à la CNIL si les dispositions sont relatives au traitement de DACP[2132]. Néanmoins, l'absence d'uniformité de la qualité des études d'impact et le manque de temps accordé à l'examen du texte par les membres du Parlement font que ces mesures se révèlent insuffisantes en pratique[2133]. Enfin, ces études d'impact devraient prendre en considération les évaluations issues de la phase de validation du SIA fournies par les concepteurs. La documentation technique relative à la conception du SIA ainsi qu'à l'ajustement de ses paramètres peut être intégrée dans l'étude d'impact facilitant ainsi la compréhension de son

---

[2129] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 246.

[2130] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 56.

[2131] Constitution de 1958, art. 39, al. 5 : « Dans les conditions prévues par la loi, le président d'une assemblée peut soumettre pour avis au Conseil d'État, avant son examen en commission, une proposition de loi déposée par l'un des membres de cette assemblée, sauf si ce dernier s'y oppose » ; LIL, art. 8 4° a) : La CNIL « peut être consultée par le président de l'Assemblée nationale, par le président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat ainsi qu'à la demande d'un président de groupe parlementaire sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données ».

[2132] Constitution de 1958, art. 39, al. 2 : « Les projets de loi sont délibérés en conseil des ministres après avis du Conseil d'État et déposés sur le bureau de l'une des deux assemblées » ; LIL, art. 8 4° a) : La CNIL « est consultée sur tout projet de loi ou de décret ou toute disposition de projet de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données ».

[2133] CESE, Rapport sur « Étude d'impact, mieux évaluer pour mieux légiférer » remis par CABRESPINES (J-L.), 2019 (mis à jour le 28 juillet 2020), 90 p., spéc. p. 51 [en ligne] :

fonctionnement et favorisant la confiance tant des utilisateurs que des personnes pouvant être concernées par le traitement des DACP[2134].

732. D'une manière générale, le contrôle assuré tout au long de la vie du SIA doit faire apparaitre les éventuels effets négatifs qu'il produit et qui n'avaient pas été identifiés lors de la phase d'évaluation. Lorsque de tels effets ont été constatés, il conviendrait qu'une nouvelle étude d'impact soit conduite afin d'améliorer le SIA et, dans le cas où ces effets seraient particulièrement graves de pouvoir soumettre de nouveau au débat la légitimité de son utilisation[2135]. L'effectivité des garanties apportées par ces mesures techniques et organisationnelles ne peut cependant être assurée sans la mise en œuvre de procédures strictes et l'intervention d'autorités de contrôle du recours aux technologies de surveillance « augmentées » de sécurité publique.

B. Le renouvellement du contrôle des technologies de surveillance « augmentées » de sécurité publique

733. Le respect des droit et libertés suppose que le recours à des technologies de surveillance « augmentées » de sécurité publique fasse l'objet d'un contrôle. Ce contrôle devrait avoir lieu tout au long du cycle de vie de ces technologies. En d'autres termes, elles doivent faire l'objet d'un contrôle *a priori* et *a posteriori* par les autorités compétentes au même titre que pour la vidéoprotection « simple »[2136]. Face aux enjeux que soulèvent les technologies de surveillance « augmentées » de sécurité publique, il est nécessaire de renforcer les procédures administratives, d'une part (1), ainsi que les moyens des autorités de contrôle auxquelles sont attribuées de nouvelles compétences, d'autre part (2).

[2134] Cependant, il convient de noter que les mesures techniques mises en œuvre par les concepteurs en faveur de l'innovation plus responsable sont susceptibles d'évoluer avec le temps (amélioration de l'état de l'art et identification des risques) et devront donc être réévaluées tout au long du cycle de vie du SIA.

[2135] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 250.

[2136] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 83 : « Il en va de "la démocratie technologique" qui se construira ainsi par l'élaboration d'un régime de transparence et de recevabilité algorithmique forte » propos de Caroline Lequesne-Roth.

1. Une modernisation des procédures administratives de déploiement des technologies de surveillance « augmentées » de sécurité publique

734. Le recours à des caméras (fixes ou mobiles) de vidéoprotection est conditionné par une autorisation du préfet territorialement compétent dans le cadre des activités de police administrative[2137] ou d'un magistrat dans le cadre des activités de police judiciaire[2138]. Il suppose aussi la mise en œuvre d'une analyse d'impact sur la protection des données remise à la CNIL[2139]. Le Sénat envisageait de fixer des exigences similaires en matière de déploiement des technologies de surveillance « augmentées » de sécurité publique[2140]. Toutefois, compte tenu des potentialités d'atteinte aux droits et libertés que présente l'utilisation de drones aériens « augmentés », il serait sans doute souhaitable que ces autorisations relèvent de la compétence d'un magistrat qu'il s'agisse d'une activité de police judiciaire ou d'une activité de police administrative[2141]. Néanmoins, dans une perspective d'amélioration de la transparence de l'usage de technologies de surveillance « augmentées » de sécurité publique, le Sénat préconisait la mise en œuvre d'un recensement national des autorisations de déploiement de ces technologies, qu'elles émanent d'un préfet ou d'un magistrat[2142].

735. Les drones aériens de sécurité publique ne font pas l'objet d'un examen préalable d'une commission départementale de vidéoprotection tel que prévu pour les caméras fixes[2143] mais sont soumis à l'avis de la CNIL préalablement à toute publication du décret autorisant leur utilisation[2144]. Dès lors, il serait aisément envisageable de confier le pouvoir de contrôle à la CNIL s'agissant des

---

2137 CSI, art. L. 252-1 et L. 242-5.

2138 CPP, art. 706-96-1 et art. 230-48.

2139 RGPD, art. 35 §3 c) et 36 ; DPJ, art. 27 §1 ; LIL, art. 90.

2140 Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 83.

2141 En ce sens, le professeur Jacques Buisson affirmait s'agissant de l'autorisation d'emploi de drones aériens (non-augmentés) à des fins de police administrative que « si ladite autorisation pouvait entrer dans la compétence du préfet puisqu'elle gouverne une activité initialement de police administrative, il eut sans doute été opportun d'en confier la délivrance à l'autorité judiciaire dès lors qu'était en cause une activité de police administrative matérielle » (BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *op. cit.*, p. 14).

2142 Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, pp. 83-84.

2143 CSI, L. 251-4.

2144 CSI, art. L. 242-8.

drones aériens « augmentés » de sécurité publique.

736. En outre, de nouveaux modes de contrôle pourraient être introduits. En premier lieu, un contrôle *a posteriori* des technologies de surveillance « augmentées » de sécurité publique pourrait être réalisé par l'intermédiaire d'un référent membre du Conseil d'État[2145] qui veillerait au respect des dispositions légales par les forces de l'ordre de l'emploi de cette technologie. Ce référent serait nommé sur le modèle de celui assigné au contrôle des fichiers de police GIPASP et PASP relatifs à la prévention des atteintes à la sécurité publique et ses fonctions seraient inscrites dans le CSI. En deuxième lieu, il pourrait être envisagé de désigner, au sein du ministère de l'Intérieur, un commissaire qui assurerait le respect des règles relatives à la captation et à l'analyse de données par des caméras de surveillance « augmentées » de sécurité publique par les forces de l'ordre, sur le modèle de celui instauré par le *Protection of Freedom Act* de 2012[2146] au Royaume-Uni.

737. Enfin, dans son rapport sur les polices municipales, la Cour des comptes avait une nouvelle fois souligné l'absence de démonstration de l'efficacité des systèmes de vidéoprotection compte tenu de leurs coûts[2147]. Elle avait ainsi recommandé que ces technologies fassent l'objet d'évaluations de leur efficacité impliquant les forces de l'ordre mais également des chercheurs et des experts reconnus. Dans le même sens, le Sénat avait recommandé la mise en œuvre d'une « évaluation publique et indépendante de l'efficacité de la technologie employée par un comité de scientifiques et de personnes qualifiées en matière d'éthique pour vérifier au cas par cas l'apport de la technologie […], sa proportionnalité, l'explicabilité de ses résultats, etc. »[2148]. Ce comité aurait notamment pour mission de formuler des propositions d'amélioration du cadre juridique, d'effectuer des recommandations, d'assurer la transparence des usages de cette technologie ainsi que d'émettre des avis.

738. Aussi, l'exécution des mesures techniques et organisationnelles permettant la maitrise des SIA et l'application effective des règles juridiques y afférents par les services de sécurité publique devront faire l'objet d'un contrôle tant par les autorités juridictionnelles que non-

---

[2145] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 57.

[2146] *Protection of Freedom Act*, 2012, section 34 [en ligne].

[2147] Cour des comptes, « Rapport : Les polices municipales », *op. cit.*, pp. 69-71.

[2148] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 81.

juridictionnelles. Or, la CNIL, qui assure le contrôle (non-juridictionnel) des traitements de DACP, souffre d'une insuffisance de ressources et l'accroissement prévu du nombre de ses compétences exige l'octroi de nouveaux moyens en vue de maintenir un niveau de contrôle satisfaisant.

2. Le renforcement des moyens mis à la disposition des autorités de contrôle du recours aux technologies de surveillance « augmentées » de sécurité publique

739. Selon la catégorie dans laquelle se place un SIA, différentes obligations s'imposeront à leurs concepteurs, qu'ils soient établis sur le territoire de l'UE ou hors de l'UE. Dans le cadre du REIA, les institutions européennes prévoient un système multi-niveaux de gouvernance reposant sur le CEIA[2149]. Ce comité est composé d'un représentant par État membre, de l'autorité de protection des données personnelles de l'UE et d'un représentant de la Commission européenne, d'une part, et d'autorités nationales afin d'assurer le respect des règles du REIA, d'autre part[2150].

740. Le REIA prévoit que chaque État membre désigne une autorité nationale de contrôle, chargée de l'implémentation et du contrôle de l'application du REIA ainsi que du rôle de point de contact unique auprès des autorités européennes et de représentant de l'État membre au sein du CEIA[2151]. Cette mission d'une autorité nationale de contrôle pourrait être assurée soit par une autorité déjà en place, par la création d'un service dédié, soit par une nouvelle autorité. Néanmoins, la création d'une nouvelle autorité est critiquable à deux endroits. D'une part, elle engendre des surcoûts liés à sa mise en œuvre ainsi qu'à son fonctionnement et est source de complexifications institutionnelles dans la mesure où cette autorité de contrôle est supposée assurer la liaison avec d'autres autorités nationales et européennes[2152]. Aussi, si le renforcement du contrôle de l'emploi de technologies ayant une incidence sur les droits et libertés revêt une importance capitale, il conviendrait d'éviter de procéder à une « multiplication des structures techniques redondantes des organes de contrôle, autrement dit, par de la complexité organisationnelle »[2153]. D'autre part, la plupart des SIA, plus particulièrement ceux utilisés par les forces de l'ordre, effectuent des

[2149] REIA, art. 56 et suiv.

[2150] REIA, art. 57.

[2151] REIA, art. 30 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 200.

[2152] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 201.

[2153] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 107.

traitements de DACP dont le contrôle relève de la compétence de la CNIL. Dès lors, le choix de cette dernière comme autorité de régulation des SIA semble naturellement s'imposer.

741. À cette fin, la CNIL avait annoncé la création de sa section « Intelligence artificielle », le 23 janvier 2023[2154], se préparant à devenir l'organisme compétent en matière de contrôle de la mise en œuvre et des usages de technologies reposant sur des SIA tel que prévu par l'article 59 du REIA. La CNIL devra donc remplir le rôle d'autorité de coordination, de supervision et de représentation auprès des institutions européennes en matière de contrôle des SIA. Son rôle se justifie pleinement dans la mesure où les fonctions de contrôle envisagées par le REIA requièrent un haut niveau de maitrise des SIA ainsi que des secteurs dans lesquels ils seront déployés[2155]. Toutefois, la CNIL pourrait exercer ses fonctions en étroite collaboration avec d'autres autorités nationales de régulation telles que le Pôle d'expertise de la régulation numérique qui assurerait le rôle d'appui technique dans ses tâches[2156].

742. À cette fin, il convient donc de réaffirmer le rôle de la CNIL en tant qu'autorité de contrôle *a posteriori* de l'adéquation à la réglementation des usages des technologies de surveillance de sécurité publique qui intégreront des SIA et du respect des finalités définies par l'autorisation de leur recours. Néanmoins, ces compétences étendues requièrent des moyens humains, techniques, financiers et institutionnels adaptés afin d'opérer les contrôles nécessaires, d'imposer les éventuels correctifs et de sanctionner les usages illégaux. En ce sens, le RGPD prévoit que « chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs »[2157]. Dans le même sens, la CJUE avait insisté, dans d'une décision du 16 octobre 2012, sur l'importance que revêtait l'octroi de moyens matériels et humains aux autorités de contrôle[2158].

2154 CNIL, « Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage », *cnil.fr*, 23 janvier 2023 [en ligne].

2155 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 201.

2156 Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 84.

2157 RGPD, art. 52 §4.

2158 CJUE, gr. ch., 16 octobre 2012, *Commission européenne c. République d'Autriche*, aff. C-614/10, §58 [en ligne].

743. Dès lors, l'attribution des compétences d'autorité de contrôle des SIA à la CNIL suppose une transformation en profondeur afin de lui octroyer les moyens nécessaires pour remplir ses nouvelles missions[2159]. Or, la situation actuelle de la CNIL n'est pas satisfaisante, qu'il s'agisse de ses ressources humaines ou financières[2160]. Ainsi, en matière de ressources financières, le rapport émis par l'*Irish Council for Civil Liberties* (ICCL) de mai 2023 fait état d'une augmentation des budgets des autorités de contrôle de protection des DACP de 12% en 2022 et place l'autorité française au quatrième rang des autorités disposant du meilleur budget au sein de l'Union européenne[2161]. Toutefois, celle-ci dispose d'un budget nettement moins conséquent que celui octroyé à l'autorité de contrôle allemande[2162] et d'un budget inférieur de moitié que l'Italie pour une population équivalente[2163]. En ce sens, le Conseil d'État regrettait que le budget alloué à la CNIL soit resté très en-deçà des besoins requis et préconisait un « investissement immédiat massif et déterminé pour augmenter les capacités du régulateur »[2164]. L'EDPB avait également publié, en septembre 2022, une étude des ressources allouées aux différentes autorités de contrôle de protection des DACP des États membres et faisait état d'une insuffisance de moyens tant financiers qu'humains pour une grande majorité des autorités de contrôle de protection des DACP des États membres de l'UE[2165].

[2159] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 58.

[2160] *Idem* : « Les effectifs de la CNIL sont aujourd'hui en-deçà de ce qui serait nécessaire, pour absorber l'ensemble des missions qui lui ont été confiées par le législateur national et européen ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 202 : « Il y a lieu de changer d'échelle en ce qui concerne les moyens, en particulier humains, accordée à [la CNIL] ».

[2161] ICCL, ICCL's 2023 report on EEA data protection authorities, May 31st 2023, p. 7 [en ligne].

[2162] En 2022, l'autorité de contrôle allemande disposait d'un budget de 104 millions d'euros pour une population d'environ 83 millions d'habitants et la CNIL d'un budget d'un peu moins de 24 millions d'euros pour une population d'environ 67 millions d'habitants [source : ICCL, p. 7].

[2163] En 2022, l'autorité italienne a bénéficié d'un budget de 44 millions d'euros pour une population d'environ 60 millions d'habitants [source : ICCL, p. 7]

[2164] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 202. Dans le même sens, le Conseiller d'État Jean-Luc Sauron remarquait déjà en 2021 que « plus que les budgets, les moyens humains sont très insuffisants compte tenu du haut niveau technologique des principaux acteurs du domaine et de la nécessité d'anticiper les mutations techniques et scientifiques régulières qui caractérisent le domaine de la protection des données » (SAURON (J-L.), « Les autorités de contrôles de protection des données un point d'étape de leurs moyens et de leur pratique », *op. cit.*, pp. 36-41, spéc. p. 41).

[2165] EDPB, « Overview on resources made available by Member States to the Data Protection Supervisory Authorities », September 5th 2022, p. 5 et p. 8 [en ligne].

744. Dans son rapport annuel de 2022, la CNIL a effectué un état de ses ressources humaines en 2022[2166] qui se révèlent encore nettement insuffisantes notamment en comparaison de l'Allemagne[2167]. Dès lors, les besoins en ressources humaines de la CNIL devront être réévalués à la hauteur des besoins que requerront les technologies de surveillance « augmentées » de sécurité publique, notamment lorsque les autorités publiques mettront en œuvre des expérimentations[2168]. Aussi, l'image de la CNIL doit évaluer pour passer de celle d'autorité de protection de la vie privée des personnes à celle de régulateur des outils numériques permettant d'assurer le respect des droits et libertés et de faciliter l'innovation technologique[2169].

745. À cette fin, plusieurs modifications doivent être apportées à la CNIL à commencer par la structure du collège qui doit intégrer de nouveaux membres spécialisés dans le domaine des SIA ainsi que d'autres acteurs issus du milieu de l'innovation[2170]. Il conviendrait également que l'autorité diversifie ses profils tant s'agissant des disciplines que de l'ancienneté de ses agents (juniors et seniors). Enfin, les différents rapports et observations font apparaitre un besoin urgent d'allouer des moyens supplémentaires à la CNIL afin qu'elle puisse assurer ses nouvelles fonctions d'autorité de contrôle des SIA plus généralement de renforcer ses fonctions d'accompagnement des acteurs dans leur procédure de mise en conformité avec le REIA et les règles relatives à la protection des DACP.

746. Indépendamment de la nécessité d'assurer un contrôle juridique et technique de la conception et de l'usage des technologies de surveillance « augmentées » de sécurité publique, leur recours nécessite une « maîtrise » tant de leur développement que de leur fonctionnement, par les autorités publiques mais aussi par les personnes faisant l'objet d'une décision à l'appui de cette technologie.

2166 CNIL, Rapport annuel de 2022 « Agir pour un futur numérique responsable », mai 2023, *op. cit.*, p. 11 : En 2022, la CNIL recensait un total de 270 agents dont 82 % de catégorie A. Elle aurait connu une hausse de 61 % de ses effectifs entre 2017 et 2022, et ses agents auraient une moyenne d'ancienneté de sept ans et cinq mois.

2167 L'autorité allemande disposait déjà de 1004 agents en 2020 et en comprenait 1155 en 2022 [source : EDPB, p. 6].

2168 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 59.

2169 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 202.

2170 *Ibid*.

Section 2 Une nécessaire « maitrise » des technologies de surveillance « augmentées » de sécurité publique

747. Les technologies de surveillance « augmentées » de sécurité publique ont fait apparaitre des enjeux en termes de compréhension de leur fonctionnement par les différents acteurs impliqués. Une des principales préoccupations repose ainsi sur la difficulté voire l'impossibilité pour une personne de comprendre les raisons qui ont conduit aux résultats produits par un SIA. Les personnes qui font l'objet d'une décision disposent pourtant d'un droit de connaitre les fondements sur lesquels ont reposé celle-ci. De même, les personnes qui endossent la responsabilité des décisions doivent pouvoir exiger des explications quant au fonctionnement du SIA de la part des concepteurs, y compris lorsque l'outil n'a qu'une vocation d'aide à la prise de décisions. En outre, l'acceptabilité sociétale du recours à cette technologie suppose de pouvoir garantir dès la conception que les éléments qui composent le SIA utilisé à des fins de sécurité publique respectent les valeurs de l'État qui en a l'usage. En d'autres termes, les concepteurs et les utilisateurs doivent s'assurer que cette technologie préserve l'autonomie et la souveraineté de l'État.

748. L'introduction des SIA au sein du secteur public tend à accroitre la méfiance que suscitait déjà l'emploi de nouvelles technologies par les forces de l'ordre. La complexité de cette technologie engendre des inquiétudes légitimes de voir apparaître des décisions préjudiciables à l'encontre des personnes surveillées, induites par une insuffisante maitrise de leurs règles techniques par ses utilisateurs. Il est alors primordial d'adopter des moyens permettant aux agents de conserver leur plein pouvoir décisionnel lorsqu'ils ont recours à des technologies de surveillance « augmentées » de sécurité publique. Aussi, face aux menaces qui planent sur les outils numériques, les différents acteurs impliqués ont pour obligation de mettre en œuvre des moyens techniques et organisationnels permettant d'assurer la sécurité de ces technologies dès la conception et tout au long de leur cycle de vie. Dès lors, la « maitrise » des technologies de surveillance « augmentées » de sécurité publique doit être entendue comme l'ensemble des mesures mises en œuvre afin de garantir de manière effective un déploiement de cette technologie dans le respect des droits et libertés (§1), d'une part, et une supervision humaine dès la conception (§2), d'autre part.

§1. Les mesures pour garantir dès la conception des technologies de surveillance « augmentées » de sécurité publique respectueuses des droits et libertés

749. Le recours à des technologies de surveillance « augmentées » de sécurité publique nécessite une information et une compréhension suffisante de leur fonctionnement par tous les acteurs impliqués. Dès lors, ces technologies doivent répondre à des exigences de transparence et d'explicabilité (A). Aussi, ces exigences vont de pair avec la protection de l'autonomie et de la souveraineté des SIA à l'usage des autorités publiques qui permettent d'assurer la continuité du contrôle de ces technologies (B).

A. Le besoin de réduire l'opacité entourant les technologies de surveillance « augmentées » de sécurité publique et favoriser leur intelligibilité

750. Ces dernières années, la France a vu apparaitre une forme de défiance à l'égard des forces de l'ordre, qu'il s'agisse de ses pratiques en matière de recours à certaines armes, telles que les lanceurs de balles de défenses (LBD), mais aussi de l'emploi de certaines technologies de surveillance au sein de l'espace public[2171]. En juin 2022, le baromètre de la confiance politique conduit par le Cevipof indiquait que 74% des sondés déclaraient avoir confiance dans la police nationale et 81% avaient confiance dans la gendarmerie nationale[2172]. Ces sondages pourraient laisser planer un doute quant à la véritable confiance accordée par l'opinion publique aux forces de l'ordre, qui se révèle être assez contrastée et en vérité plutôt méfiante notamment s'agissant des usages technologiques[2173].

751. Face à la défiance de l'opinion public pour l'emploi de nouvelles technologies par les forces de l'ordre, l'introduction des technologies de surveillance « augmentées » de sécurité publique doit ainsi prendre en considération cet état de fait et adopter des mesures favorisant la

---

2171 AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, spéc. pp. 97-98.

2172 Sciences Po (Cevipof), « En qu(o)i les Français ont-ils confiance aujourd'hui ? », *Le baromètre de la confiance politique - vague 13b*, juin 2022, p. 35 [en ligne].

2173 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 48 : « Aujourd'hui, on constate une accentuation de la défiance envers les technologies, lorsqu'elles sont employées dans le champ de la sécurité. Une frange de la société civile est clairement hostile à l'emploi des technologies par les forces de sécurité intérieure. Parmi elles, les associations protectrices des droits et de l'Homme critiquent l'augmentation croissante des atteintes à la vie privée, ainsi que le recours accru aux technologies à des fins de surveillance des populations ». Voir notamment en ce sens : La Quadrature du Net, « Technopolice » [en ligne] ; EDRi, « Surveillance and data retention » [en ligne].

transparence de leur fonctionnement et de leurs usages à la hauteur des enjeux. Ce concept de transparence (à l'opposé de celui d'opacité) comprend deux visées distinctes mais complémentaires : une visée descriptive et une visée prescriptive[2174]. La finalité descriptive repose sur le fait de vouloir rendre explicable et intelligible le fonctionnement d'un algorithme au travers de procédés mathématiques et informatiques (1). La finalité prescriptive fait référence aux normes et aux principes juridiques et éthiques telles que la loyauté et l'équité (2).

1. L'interprétabilité et l'explicabilité des SIA utilisés à des fins de sécurité publique

752. L'intérêt pour les SIA s'explique avant tout par les performances plutôt convaincantes de certains algorithmes reposant sur des réseaux de neurones, notamment en matière de reconnaissance et d'analyse d'images[2175]. Cependant, leur complexité tend à faire apparaitre un phénomène d'opacité, dit de « boîte noire », qui repose sur une incapacité humaine à comprendre le raisonnement ayant conduit le SIA à produire ces résultats à partir des données d'entrée. Or, ce phénomène n'affecte pas uniquement les utilisateurs mais peut également concerner les concepteurs eux-mêmes. Cette opacité des algorithmes complexes serait directement liée à la façon dont fonctionnent les réseaux de neurones[2176] qui effectuent des corrélations ou des inférences[2177]. En d'autres termes, leurs résultats reposent sur des probabilités et non sur des causalités qui permettraient pourtant de mieux discerner la logique des résultats obtenus[2178]. Or, l'opacité susceptible d'entourer les technologies de surveillance « augmentées » de sécurité publique pourrait porter atteinte à la liberté individuelle, dans la mesure où les décisions prises à l'aide du SAAD ne seraient pas entièrement explicables. Les inquiétudes concernant l'opacité de ces SAAD se

---

2174 PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *op. cit.*, p. 9.

2175 MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 160 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 264.

2176 MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 161.

2177 En IA, l'inférence « est une opération logique basée sur l'induction. [Elle] vise à réaliser des prédictions efficaces à partir d'un modèle d'apprentissage entraîné » (CROCHET-DAMAIS (A.), « Inférence en machine learning et deep learning : définition et cas d'usage », *Journal du Net*, 8 mars 2022 [en ligne] consulté le 12 mars 2022).

2178 BASDEVANT (A.) et MIGNARD (J-P.), *L'empire des données - Essai sur la société, les algorithmes et la loi*, *op. cit.*, p. 96. Voir aussi sur les différences entre corrélation et causalité : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, pp. 166-173.

justifient d'autant plus que « la frontière entre l'aide à la décision et la décision tend parfois à se brouiller »[2179].

753. Interprétabilité et explicabilité des SIA - Dès lors, l'exigence d'explicabilité s'impose dans une perspective élargie du respect des droits et libertés. L'explicabilité prise dans son sens étendu comprend le concept d'interprétabilité, qui suppose que le responsable du SIA ait la capacité de comprendre les opérations effectuées par la machine qui l'ont conduite à ses résultats[2180]. Ce concept, issu du terme anglo-saxon d'*explainability*, est parfois désigné sous le terme d'intelligibilité[2181]. L'insuffisance d'interprétabilité à laquelle sont confrontés les concepteurs de SIA reposant sur les réseaux de neurones a suscité un important champ de recherche orienté vers le développement de méthodes favorisant la compréhension du modèle appris et des techniques expliquant leurs résultats[2182]. Aussi, ce concept d'interprétabilité est proche de celui d'explicabilité qui fait référence à l'obligation pour le concepteur d'expliquer dans un langage compréhensible aux utilisateurs finaux les éléments essentiels permettant de comprendre le cheminement mathématique adopté par le SIA pour produire ses résultats[2183].

754. L'explicabilité d'un SIA est essentielle et constitue même un critère prépondérant au sens du rapport remis par le mathématicien Cédric Villani sur l'IA[2184]. Cette exigence d'explicabilité des SIA publics revêt une importance particulière au regard de la DDHC, qui énonce que « la société a le droit de demander compte à tout agent public de son administration »[2185] et par conséquent induit une obligation pour cette dernière d'expliciter le fonctionnement des technologies dont elle a

---

2179 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 78.

2180 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 122.

2181 BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 17. Voir aussi : DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, pp. 221 et suiv. ; PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *op. cit.*, pp. 8-10.

2182 Voir notamment : Defense Advance Research Project Agency (DARPA), Project *Explainable AI* (« XAI ») [en ligne] ; SAMEK (W.) *et al.,* "Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models", August 28th 2017 [en ligne].

2183 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 122.

2184 Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, pp. 145-146.

2185 DDHC, art. 15.

l'usage[2186]. En outre, l'obligation de motivation des décisions auxquelles peut être tenue l'administration suppose d'être en mesure de fournir aux personnes concernées des explications quant aux fondements juridiques et factuels[2187] de ses décisions. L'explicabilité est donc nécessaire dans le cadre de l'usage des technologies de surveillance « augmentées » de sécurité publique à plusieurs égards. En premier lieu, l'explicabilité permet d'assurer la vérifiabilité des résultats[2188]. En ce sens, les forces de l'ordre doivent être en mesure de comprendre les résultats produits par l'algorithme et savoir quand elles ne doivent pas en tenir compte lorsque le résultat comprend une erreur ou un biais. En deuxième lieu, l'explicabilité permet de vérifier la conformité du SIA à la règlementation et aux éventuelles normes. Cette conformité suppose de pouvoir contester les résultats du SIA lorsqu'ils comprennent des erreurs ou conduisent à des discriminations. En dernier lieu, l'explicabilité permet d'assurer la confiance des individus et donc l'acceptabilité des technologies « augmentées »[2189].

755. Les formes d'explicabilité - Il existe plusieurs formes d'explications des SIA. L'explicabilité « locale » se réfère à la possibilité d'expliquer les résultats produit par l'algorithme pour un cas particulier[2190]. Elle consiste à identifier les facteurs clés qui ont conduit le SIA à produire ce résultat. Dans le cadre d'une décision prise sur le fondement d'un système de vidéoprotection « augmenté », il s'agirait de comprendre les raisons pour lesquelles parmi les différents critères ou indices permettant l'analyse d'images, le SAAD a produit le résultat ayant conduit à une alerte ou au contraire à ne pas produire d'alerte sur base de différents critères qu'il a reconnu comme décisifs.

[2186] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 123.

[2187] Code des relations entre le public et l'administration (CRPA), art. L. 211-5. En ce sens, le Conseil d'État rappelait que « la connaissance des déterminants de la décision est une condition d'effectivité du contrôle de l'erreur de droit, permettant de détecter une méconnaissance de la loi voire des biais discriminatoires » (*Ibid*).

[2188] BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 17.

[2189] *Ibid* ; JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 90.

[2190] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 222 ; CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 122.

756. L'explicabilité « globale » est celle du fonctionnement ou de la logique générale du SIA[2191]. En d'autres termes, elle permet de comprendre les résultats du SIA pour l'ensemble des données et donc pour tout type de situation[2192]. Elle permet d'interpréter l'ensemble des résultats d'un SIA. Les différentes formes d'explications existantes peuvent dépendre du type de données traitées par l'algorithme, du domaine auquel il se destine ou encore les finalités des utilisateurs. Aussi, ces explications comprennent toutes des limites et il n'existe pas de forme d'explication générale pour tous les algorithmes.

757. Élargir l'explicabilité - Aussi, il est légitime pour toute personne concernée par le traitement d'un SIA public d'exiger une explicabilité minimale. Toutefois, il ne peut être raisonnablement demandé d'être en mesure de fournir une explicabilité « totale » du SIA comme condition à leur recours puisqu'il n'existe aucun standard d'explicabilité possiblement applicable à tous les SIA. Dès lors, l'exigence d'explicabilité devrait prendre en compte plusieurs considérations. Tout d'abord, cette exigence devrait être proportionnée au niveau potentiel d'atteinte aux droits et libertés par le SIA. Ensuite, il parait nécessaire d'effectuer une conciliation entre les apports du SIA aux missions de sécurité publique, d'une part, et les inconvénients d'une explicabilité insuffisante du fait de la complexité de l'algorithme, d'autre part. Enfin, il importe moins de définir un standard d'explicabilité que de s'assurer que les personnes concernées par la décision ont reçu une explication en adéquation avec leur niveau de compétence et la gravité de l'atteinte[2193].

758. Il convient de souligner que le REIA ne fait pas mention de l'exigence d'explicabilité, à l'exception d'un considérant consacré aux SIA à des fins répressives[2194]. Il se limite à imposer un fonctionnement transparent des SIA à haut risque afin que les utilisateurs puissent interpréter les résultats et en faire un usage approprié[2195]. Dès lors, le REIA limite l'exigence de transparence à

2191 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 222.

2192 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 123.

2193 *Idem*, p. 124.

2194 REIA, cons. 38.

2195 REIA, art. 13 §1 : « La conception et le développement des systèmes d'IA à haut risque sont tels que le fonctionnement de ces systèmes est suffisamment transparent pour permettre aux utilisateurs d'interpréter les résultats du système et de l'utiliser de manière appropriée ».

l'égard des destinataires de la décision à la seule information du recours à un SIA à haut risque et non à son explicabilité.

759. Enfin, plusieurs questions restent en suspens s'agissant de l'explicabilité des technologies de surveillance « augmentées » de sécurité publique. D'une part, l'exigence d'explicabilité se confronte à celle de performance, dans la mesure où les recherches menées dans ce domaine ont démontré que plus les méthodes algorithmiques sont performantes moins elles sont transparentes et inversement les méthodes les plus transparentes peinent à assurer une précision suffisante[2196]. Dès lors, la conciliation entre l'exigence de performance des services de l'État et celle de transparence à l'égard des destinataires des décisions rendues au moyen d'un SIA reste à opérer[2197]. D'autre part, la diversité des formes d'explicabilité ne permet pas d'adopter un modèle standardisé qui déterminerait le contenu et la forme de l'explicabilité à délivrer en fonction des destinataires. Aussi, le concept général de transparence comprend une notion plus spécifique d'information et de loyauté quant à l'usage d'un SIA.

2. La transparence des SIA à des fins de sécurité publique

760. En l'absence d'informations transparentes permettant de savoir si une technologie repose sur un SIA et, auquel cas, sur quels critères reposent les résultats de ce dernier, il se révèle difficile voire impossible de pouvoir contester une décision ayant causé un préjudice[2198]. L'exigence de transparence est ainsi essentielle afin de garantir le respect des droits et libertés. Compte tenu des potentialités d'atteintes aux droits et libertés que présentent les technologies de surveillance « augmentées » de sécurité publique, il sera impératif d'informer les personnes concernées de l'existence du traitement qu'elles opèrent. En ce sens, la LIL pose le principe selon lequel « la personne concernée justifiant de son identité a le droit d'obtenir […] les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise

---

2196 BOLOGNA (G.) and HAYASHI (Y.), "Characterization of symbolic rules embedded in deep dimlp networks: A challenge to transparency of deep learning", *Journal of Artificial Intelligence and Soft Computing Research* n°4, Vol. 7, 2017, pp. 265-286 [en ligne].

2197 MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 163 : « Les experts en métadonnées (*datascientists*) sont ainsi régulièrement conduits à devoir décider s'ils sont prêts à réduire la performance de prédiction de leur système pour obtenir une certaine forme d'explicabilité ».

2198 CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 34. Voir aussi : PASQUALE (F.), *The Black Box Society: The Secret Algorithms That Control Money and Information*, *op. cit.*

sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé »[2199]. Le principe de transparence œuvre ainsi en faveur de la confiance des individus en révélant les activités opérées par l'État en matière de traitement de DACP.

761. En France, la transparence des informations numérisées tire son fondement de la loi du 17 juillet 1978[2200] permettant l'accès aux documents administratifs auprès de la Commission d'accès aux documents administratifs (CADA). Ces mesures de transparence ont par la suite été étendues par la loi pour une République numérique du 7 octobre 2016[2201]. Dès lors, en matière de SIA publics, ces dispositions confèrent en principe un droit pour toute personne d'accéder aux documents décrivant les éléments-clés sur lesquels reposent les systèmes utilisés. Le recours à des technologies de surveillance « augmentées » de sécurité publique entreraient par conséquent dans le champ du droit à la communication des documents administratifs[2202]. Cependant, la communication de ces documents est soumise à deux conditions. En premier lieu, la publication des documents relatifs au SIA public ne doit pas être obérée par des droits de propriété intellectuelle de tiers (secret des affaires)[2203]. En deuxième lieu, les documents concernant ce SIA ne doivent pas être soumis au secret protégé par la loi. En ce sens, il convient de rappeler que l'exigence de transparence ne peut faire obstacle au principe de confidentialité exigé dans le cadre de certaines activités, notamment celles relatives à la sécurité de l'État (défense) ou encore à la sécurité publique[2204]. Dès lors, ces domaines font l'objet de dérogations quant à l'exigence de transparence à l'égard du public (transparence limitée), à l'exception des autorités de contrôle compétente pour qui l'exigence de

---

[2199] LIL, art. 119 II 5).

[2200] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, dite « loi CADA », *JORF* du 18 juillet 1978 [en ligne] : cette loi s'inscrit dans la droite lignée de la LIL (adoptée en janvier 1978) permettant déjà l'octroi d'une forme de contrôle des administrés sur les documents administratifs dématérialisés.

[2201] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *op. cit*.

[2202] CRPA, art. L. 311-2.

[2203] Voir sur ce sujet la décision du Tribunal de première instance de l'UE (TPIUE) concernant la communicabilité de documents relatifs à un projet de SIA avec pour finalité la détection de fausses déclarations aux frontières extérieures de l'UE (TPIUE, 15 décembre 2021, *Breyer c. Agence exécutive européenne pour la recherche*, aff. T-158/19 [en ligne]).

[2204] CRPA, art. L. 311-5. Le professeur Bertrand Warusfel précise ainsi que la Commission d'accès aux documents administratifs (CADA) peut refuser la communication de documents dans le domaine de la sécurité publique « dont la divulgation serait de nature à lui porter atteinte » (WARUSFEL (B.), « Enjeux et limites de l'ouverture des données en matière de sécurité et de défense », *Revue française d'administration publique* n° 167, mars 2018).

transparence s'applique de manière stricte[2205].

762. Plusieurs chercheurs sont favorables à la transparence des algorithmes[2206]. Néanmoins, il ne faudrait pas que cette transparence se limite à la communication du code source. En ce sens, le Parlement européen avait admis que « la divulgation du code informatique lui-même ne résoudra pas le problème de la transparence de l'IA parce qu'il ne révélerait pas les biais inhérents qui existent et ne permettrait pas d'expliquer le processus d'apprentissage automatique »[2207]. En outre, la publication du code ne présente que peu d'utilité compte tenu du fait qu'il reste hors de portée de la compréhension par tous[2208]. En ce sens, le Conseil d'État soulignait « l'inaccessibilité des codes-sources à l'entendement du citoyen non expert [ainsi que] la difficulté pour la personne concernée à percevoir l'intérêt que présente pour elle le développement d'un SIA et le profit qu'elle peut en retirer personnellement, à supposer qu'il ne soit pas conçu pour prendre des décisions défavorables à son égard »[2209]. Les informations communiquées doivent donc être adaptées tant au contexte qu'au public visé[2210].

763. Cette exigence de transparence s'impose de prime abord à l'égard des utilisateurs. Dès lors, les autorités publiques devront disposer d'informations suffisantes concernant les caractéristiques du SIA équipants les technologies de surveillance. En ce sens, le REIA comprend une obligation à l'égard des concepteurs de SIA à haut risque de fournir une notice d'utilisation compréhensible comprenant les caractéristiques, les capacités et les limites du système[2211]. En deuxième lieu, le principe de transparence s'adresse aussi et avant tout aux personnes sur lesquelles

---

2205 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 120.

2206 Voir en ce sens : KEATS CITRON (D.) and PASQUALE (F.), "The Scored Society: Due Process for Automated Predictions", *Washington Law Review*, Vol. 89, April 23rd 2014 [en ligne].

2207 Parlement européen, Résolution sur « Une politique industrielle européenne globale sur l'intelligence artificielle et la robotique », 12 février 2019 (2018/2088(INI)), p. 27 §166 [en ligne].

2208 CHANDER (A.), "The Racist Algorithm?", *Michigan Law Review*, Vol. 115, 2017, pp. 1023-1045, p. 1040 [en ligne]. Voir aussi : DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 222.

2209 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 143.

2210 CAHAI du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », *op. cit.*, p. 35.

2211 REIA, art. 13 §2 : « Les systèmes d'IA à haut risque sont accompagnés d'une notice d'utilisation dans un format numérique approprié ou autre, comprenant des informations concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les utilisateurs ».

porteront une part des décisions des technologies de surveillance « augmentées » de sécurité publique. Ce principe comporte notamment une exigence de transparence qui impose au responsable du système d'informer les personnes concernées par le traitement du SIA lorsque ce dernier a conduit à une décision portée à son encontre. L'administration doit ainsi respecter une obligation d'information générale du public. Or, il est possible de s'interroger sur l'effectivité de cette garantie compte tenu des pratiques constatées[2212]. Aux fins de pallier cette opacité des usages technologiques par l'administration, il convient d'imposer à celle-ci d'informer le plus en amont possible de ses intentions et objectifs s'agissant du recours à de nouvelles technologies. En outre, elle devra démontrer les raisons et la nécessité pour lesquelles elle souhaite faire usage de ces technologies. La transparence de l'usage de ces technologies « augmentées » permet de renforcer la confiance du public et est ainsi un gage d'acceptabilité sociétale[2213].

764. Enfin, cette exigence de transparence doit s'accompagner d'une garantie d'auditabilité du système aux fins de nuancer l'insuffisance d'explicabilité des résultats de certains SIA du fait de leur complexité[2214]. À cette fin, les étapes de développement, les choix de conception, les jeux de données ainsi que les divers processus utilisés devront être documentés pour permettre aux autorités indépendantes compétentes d'auditer le processus d'apprentissage ainsi que les résultats qu'ils produisent[2215]. Aussi, l'auditabilité de ces technologies se conjugue avec les besoins d'assurer l'autonomie et la souveraineté des outils à l'usage de l'État.

B. Une stratégie de développement des technologies de surveillance « augmentées » de sécurité publique préservant l'autonomie et la souveraineté de l'État

765. Les technologies à l'usage de la sécurité publique ont complexifié la relation de confiance établie entre le grand public et les forces de l'ordre. Indépendamment de l'enjeu de surveillance, la provenance de ces outils et le manque de maitrise des autorités françaises sur ceux-

---

2212 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 121. Ici encore, l'utilisation illégale de drones aériens par des forces de l'ordre à Paris en 2020 ainsi que la tenue illégale de fichiers de police incitent à la méfiance.

2213 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 51.

2214 Voir notamment : SANDVIG (K.) *et al.*, "Auditing algorithms: Research methods for detecting discrimination on internet platforms", *64th Annual Meeting of the International Communication Association*, May 22nd 2014 [en ligne] ; BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », *op. cit.*, p. 18.

2215 REIA, art. 43 ; *Idem*, p. 125.

ci engendrent des enjeux de souveraineté[2216]. En ce sens, l'absence de transparence quant à la conception d'outils, toujours développés à l'étranger et utilisés à des fins de sécurité publique conduit ainsi à une perte d'autonomie de la puissance publique en amplifiant les potentialités d'atteintes aux droits et libertés d'une technologie, de surcroît, très intrusive[2217]. En outre, le recours à des technologies issues du secteur privé présente également des enjeux d'autonomie de la puissance publique (1). Dès lors, il semble opportun de prendre en considération l'origine des éléments (nationale ou étrangère) et le type de développement (interne ou externe) des technologies de surveillance « augmentées » de sécurité publique. En ce sens, le Conseil d'État rappelait que pour maintenir « la capacité de la puissance publique à assurer ses fonctions essentielles, la stratégie de l'IA publique doit être conçue de manière à préserver la souveraineté de la France et à garantir l'autonomie de la Nation »[2218]. À cette fin, il convient de privilégier des solutions reposant sur des ressources maitrisées et souveraines (2).

1. Une nécessaire maitrise de la collaboration avec le secteur privé

766. En dépit du fait que la majorité des outils algorithmiques soient d'origine commerciale[2219], certains outils à l'usage de la sécurité publique ont été développés en interne que ce soit en France ou à l'étranger. Ces dernières années, le ministère de l'Intérieur a mis en œuvre des solutions visant à privilégier l'autonomie de la puissance publique par une maitrise du développement des technologies employées ainsi que des partenariats établis avec le secteur privé[2220]. Les technologies de sécurité publique développées en interne présentent un double avantage. D'une part, elles seraient plus adaptées aux besoins des agents et de leurs permettre une meilleure maitrise de leur fonctionnement. D'autre part, la conception effectuée en collaboration avec les services qui les utiliseront constitue un facteur non négligeable en faveur d'une plus grande

---

[2216] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 105 ; Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 220.

[2217] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 102.

[2218] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 130.

[2219] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 90 : « L'écosystème des technologies de sécurité est aujourd'hui marqué à la fois par une explosion des technologies disponibles et développées par le secteur privé ».

[2220] *Ibid*.

acceptabilité tant du grand public que de défenseurs des droits et libertés[2221]. En outre, les développements en interne présentent de meilleures garanties de protection des droits et libertés, à l'inverse des algorithmes issus du secteur privé étranger, en ce que « la loi impose à l'administration française des obligations pour les traitements automatisés de données personnelles »[2222] telles que le respect de la règlementation relative à la protection des DACP ainsi que la transparence de l'utilisation d'algorithmes.

767. Le constat d'un recours plus fréquent à des solutions commerciales par les forces de l'ordre à l'étranger[2223] plutôt qu'à des logiciels développés en interne induit des questions d'autonomie et donc de maîtrise de ces outils par les services concernés, qui n'auront pas participé à leur conception. En ce sens, la Cour des comptes avait souligné dans son rapport annuel de 2018 que l'externalisation des projets numériques comportait des avantages autant que des inconvénients[2224]. Une technologie de sécurité publique fournie par un prestataire externe présente une opportunité d'amélioration des activités mais engendre aussi des coûts de maintenance et de mise à jour parfois importants[2225]. En outre, la conception d'origine externe des outils d'aide à la décision à des fins de sécurité publique soulève des enjeux en matière de transparence des contrats publics[2226]. Néanmoins, il convient de noter que si la conception en interne des dispositifs de sécurité publique permet à leurs utilisateurs d'en assurer la maitrise, ce mode de conception présente également des contraintes en termes de ressources humaines et financières qui exigent des services

---

[2221] CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 28. : « Le déploiement d'outils internes présentent plusieurs avantages. L'un d'entre eux est sans doute une meilleure pertinence de l'outil et, partant, une meilleure acceptabilité s'il a été élaboré par les services destinés à l'utiliser ».

[2222] *Idem*, p. 34

[2223] Parmi les principaux logiciels d'IA externes commerciaux utilisés par les forces de l'ordre peuvent être cités : *PredPol*, *Palantir*, *Hunchlab* ou encore *Beware*.

[2224] Cour des comptes, Rapport public annuel sur « Amplifier la modernisation numérique de l'État », février 2018, p. 160 [en ligne] : « L'administration […] avait trop largement externalisé ses compétences informatiques au cours des vingts dernières années. L'intégration au sein de l'administration des meilleurs profils conditionne pourtant sa capacité de pilotage de la transformation numérique. Elle constitue en effet un élément essentiel du dispositif de maitrise des risques et de réduction des dépenses ».

[2225] DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 51.

[2226] CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 30 (note de bas de page 52).

concernés de disposer du personnel ayant les compétences requises afin d'assurer leur maintenance[2227].

768. Sous la pression des lobbys issus des entreprises technologiques et des exigences de la population en faveur d'une plus grande sécurisation de l'espace public, les forces de l'ordre ont déjà eu recours à des outils algorithmiques étrangers[2228]. En France, la Direction Générale de la Sécurité Intérieure (DGSI) s'était trouvée face à l'absence d'outil interne[2229] (ou même externe national[2230]) pour remplir ses missions de lutte contre le terrorisme et avait dû recourir au logiciel de la société *Palantir*[2231]. Le recours à cette solution avait suscité la controverse quant aux potentialités d'atteintes portées à la confidentialité des données, notamment des DACP sensibles, du fait de l'accès à celles-ci par les services de renseignements américains au travers d'entreprises privées[2232]. De fait, l'emploi de logiciels étrangers ne permet pas de garantir une maitrise des données collectées lorsque les entreprises dont ils proviennent sont tenues par une obligation de les transmettre aux autorités de leur État. À titre d'exemple, les entreprises américaines sont soumises à la loi extra-territoriale américaine *Clarifying Lawful Overseas Use of Data Act*[2233] ou *Cloud Act* qui prévoit la possibilité pour les autorités américaines de demander aux prestataires de communications électroniques ainsi qu'aux prestataires des services informatiques à distance, la communication des données de leurs clients, y compris lorsqu'elles ne sont pas hébergées aux États-

---

2227 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 51.

2228 AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 105 : « L'utilisation de logiciels américains ou de caméras chinoises suscite des craintes sur la maîtrise de nos propres équipements, et sur le transfert de données personnelles de Français à des pays dont le modèle en la matière est éloigné du nôtre » ; EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *op. cit.*

2229 CHEMI, Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), *op. cit.*, p. 32 (note de bas de page 58).

2230 ROSEMAIN (M.), « La DGSI renouvelle son contrat avec l'Américain Palantir, faute de système 100 % français », *L'Usine Digitale*, 27 novembre 2019 [en ligne] consulté le 15 mars 2023.

2231 Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), *op. cit.*, p. 220 ; EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *op. cit.* À noter qu'en janvier 2023, la DGSI annonçait son appel d'offre auprès de plusieurs entreprises françaises afin de remplacer la société Palentir dans la gestion de ses données (« Cloud de la DGSI : Atos ou Thales pour succéder à Palantir ? », *Siècle Digital*, 3 janvier 2023 [en ligne]).

2232 AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 106 : « Le choix de la DGSI de faire appel à la société *Palentir* comme solution de gestion de leurs flux de données a […] fait couler beaucoup d'encre du fait du risque de fuite de données sensibles, sans que la direction ne revienne sur sa décision ».

2233 The United States Department of Justice, *Clarifying Lawful Overseas Use of Data Act* (or *Cloud Act*), March 21st 2018 [en ligne].

Unis[2234]. Dès lors, l'extra-territorialité du *Cloud Act* peut laisser craindre une atteinte à la confidentialité des données[2235]. Toutefois, le propos reste à nuancer, l'application de ce texte étant, en pratique, très encadré[2236]. Néanmoins, face aux critiques légitimes formulées à l'encontre du recours par la DGSI au logiciel de *Palantir*[2237], plusieurs initiatives ont vu le jour afin de proposer des alternatives souveraines aux différents services issus du secteur public[2238]. La souveraineté technologique et l'autonomie des services de sécurité publique reposent de fait sur une maitrise des composants et de l'usage de ses technologies. Dès lors, ces services doivent sélectionner leurs dispositifs de sécurité publique auprès d'acteurs de confiance qui permettront notamment d'assurer l'intégrité des données dès la conception et d'offrir des garanties tant juridiques que techniques[2239]. En outre, l'assurance d'une souveraineté technologique des dispositifs de sécurité publique permet de répondre aux exigences en matière de maitrise des SI publics et de garantir la confidentialité des DACP collectées par l'administration[2240].

769. Au-delà de vouloir restaurer la confiance entre les citoyens et les forces de l'ordre, il s'agit également d'assurer celle du grand public envers les concepteurs des technologies de sécurité publique[2241]. En outre, l'assurance de l'autonomie des institutions françaises suppose qu'elles

---

2234 FEUTEUN (C.) et RIMSEVICA (D.), « Cloud Act et cloud computing : une menace pour les données ? », *Revue de Droit bancaire et financier* n° 5, septembre 2020, dossier 27.

2235 En l'absence d'accord bilatéral entre les États-Unis et l'Union européenne, l'*EDPB* et l'*EDPS* avaient constaté un conflit de loi entre les dispositions du *Cloud Act* et celles des articles 48 et 49 du RGPD lors de leur analyse d'impact du *Cloud Act* sur le régime européen de protection des données à caractère personnel (EDPB-EDPS, "Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection", July 12th 2019 [en ligne]).

2236 Le *Cloud Act* exige l'obtention d'un mandat, d'une injonction ou d'une ordonnance judiciaire. En outre, il octroie au prestataire un droit d'opposition à la communication des données réquisitionnées par les autorités américaines (*Cloud Act, op. cit.,* 18 U.S. Code § 2703).

2237 En 2018, le Directeur général de l'ANSSI déplorait l'usage du logiciel *Palantir* par les autorités françaises et déclarait participer activement à l'élaboration de solutions souveraines notamment dans le cadre du programme *Artemis* (AN, Compte rendu n° 53 (2017-2018) Commission de la défense nationale et des forces armées - Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire, p. 17 [en ligne]).

2238 En 2019, la société française Atos annonçait la création du consortium *Artemis*, ayant la Direction générale de l'Armement pour partenaire, dont l'objectif reposait sur le développement d'une infrastructure souveraine de stockage et de traitement massif de données [23 mai 2019 en ligne]. Dans une démarche similaire et plus générale, les sociétés françaises Atos et Thalès ont créé la société *Athea* avec pour ambition de développer une plateforme souveraine associant traitement de données massives et intelligence artificielle à destinations des secteurs de la défense, du renseignement et de la sécurité intérieure [27 mai 2021 en ligne] consulté le 15 mars 2023.

2239 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 132.

2240 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *op. cit.*, art. 16 : « Les administrations […] veillent à préserver la maîtrise, la pérennité et l'indépendance de leurs systèmes d'information ».

2241 AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 105.

puissent intervenir dans le choix des solutions qu'elles souhaitent déployer en matière de SIA. Cette stratégie d'autonomie des SIA publics induit également une maitrise de ces systèmes par les institutions françaises afin de prévenir les éventuelles atteintes portées à la Nation et aux citoyens par des institutions ou entreprises étrangères sur lesquelles elles ne peuvent exercer aucune forme de contrôle[2242]. En ce sens, le député Jean-Michel Mis préconisait le choix de « solutions souveraines pour les usages les plus critiques et dans le respect du droit de la commande publique » afin de renforcer les garanties des droits et libertés « en évitant une extra-territorialisation des flux »[2243]. À cette fin plusieurs solutions ont été proposées.

2. Les conditions nécessaires à la recherche et au développement des technologies de surveillance « augmentées » de sécurité publique garantissant la souveraineté

770. La protection de l'autonomie technologique de la France est une garantie de la sauvegarde des droits et libertés[2244]. L'autonomie technologique des forces de l'ordre suppose une liberté de choix en matière de conception des outils employés par les policiers et gendarmes nationaux. Or, cette liberté de choix ne peut être effective que dans le cas où les ressources qui permettent le développement et l'utilisation de ces technologies sont disponibles. Cette disponibilité repose tant sur la contrainte d'assurer la légalité de l'utilisation des ressources (ex. données libres de droit) que sur la richesse de celles-ci (ex. nombre, pertinence, etc.). Dès lors, plusieurs enjeux doivent être pris en compte afin d'assurer une autonomie des forces de l'ordre quant à l'utilisation de technologies de surveillance « augmentées » de sécurité publique.

771. Acteurs de la recherche et du développement - Le développement de technologies souveraines nécessite des compétences intra-étatiques. Or, la France dispose de nombreux chercheurs et experts dans le domaine des nouvelles technologies[2245]. La stratégie numérique doit donc se concentrer sur ce vivier et favoriser la mise en œuvre de projets de recherche avec les acteurs français (ou européens) en matière d'outils numériques. De même, il convient de mettre en

---

[2242] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 131.

[2243] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), op. cit., p. 43.

[2244] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 102.

[2245] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 131.

œuvre des solutions à destination des structures de recherche et de développement, principalement s'agissant des jeux de données nécessaires à l'apprentissage des algorithmes composant les SIA publics.

772. La maitrise des données d'apprentissage - La maitrise des technologies « augmentées » à des fins de sécurité publique repose avant tout sur la traçabilité des données d'apprentissage. À cette fin, il est possible de mettre en œuvre des dispositifs de certification ou de labellisation des SIA qui reposeraient sur une analyse de la provenance des données d'apprentissage[2246]. Les partenaires publics et privés qui développent des SIA doivent recourir à des jeux de données importants et suffisamment variés pour entrainer leurs algorithmes de manière à les rendre plus fiables et respectueux des principes de non-discrimination. Toutefois, l'insuffisance de disponibilité des jeux de données entravent leurs capacités de recherche et de développement des SIA. En règle générale, le RGPD dispose que tout traitement de DACP à des fins de recherche scientifique doit obligatoirement recueillir le consentement des personnes concernées[2247]. En d'autres termes, les personnes concernées devraient être informées du traitement de leurs données à des fins de recherche scientifique. Cette condition présente de solides garanties des droits pour les personnes concernées mais constitue aussi « un obstacle de taille dans la mesure où une base de données doit parfois contenir des millions d'images pour être performante »[2248]. En vue de faire face à cette difficulté, le Sénat préconisait de faciliter l'accès à des jeux de données par l'adoption de dispositions législatives autorisant la mise à disposition de DACP, y compris biométriques, traitées par des administrations aux organismes de recherche publique. Cette autorisation serait alors conditionnée par un avis favorable de la CNIL et ne pourrait être effectuée que « dans un environnement de traitement des données sécurisé, fourni par l'État et sans possibilité d'en exporter les données »[2249].

[2246] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, pp. 354-355 ; Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 106.

[2247] RGPD, cons. 33 : « Les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique » et « les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet. ».

[2248] Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 104.

[2249] *Idem*, p. 105.

773. Infrastructures et communication - La stratégie d'autonomie et de souveraineté des SIA publics concerne tant les infrastructures d'hébergement des données que les moyens de communication de l'État. S'agissant des activités de communication à des fins de sécurité publique, la LOPMI a permis d'introduire de nouvelles mesures permettant d'assurer une meilleure continuité des communications des services de sécurité et de secours[2250]. Le décret du 30 mars 2023[2251] a créé un nouvel établissement public national dénommé « Agence des communications mobiles opérationnelles de sécurité et de secours » (ACMOSS), laquelle est placée sous l'autorité du ministère de l'Intérieur. Cette nouvelle agence bénéficie de réseaux et de systèmes d'infrastructures spécifiques afin d'assurer l'acheminement en priorité des communications mobiles de services critiques[2252]. Elle s'impose comme un opérateur indépendant des communications mobiles des services de sécurité et de secours. Elle s'inscrit dans une politique de modernisation des outils à l'usage des forces de l'ordre et des services de secours et permet de garantir un accès prioritaire aux communications des services de secours en cas de congestion du réseau sur les réseaux ouverts au public.

774. Outre ses avantages sur le plan technique, l'ACMOSS symbolise une mesure permettant de s'affranchir du lien de dépendance au secteur privé et ainsi d'affirmer l'autonomie technologique de l'administration (v. n° **446 et suiv.**). L'hébergement des données constitue également un enjeu de souveraineté dans la mesure où les services de stockage en nuage (*cloud*) sont indispensables et ne devraient pas être assurés par des entreprises étrangères[2253]. Or, les SIA requièrent un service de maintenance continu qui, compte tenu de la sensibilité des informations qui peuvent être traitées par les services de l'État, devrait reposer sur des solutions souveraines[2254]. Dès lors, la localisation en

---

[2250] LOPMI, art. 11.

[2251] Décret n° 2023-225 du 30 mars 2023 portant création de l'agence des communications mobiles opérationnelles de sécurité et de secours, *JORF* n°0077 du 31 mars 2023 [en ligne].

[2252] CPCE, R. 20-29-20.

[2253] En ce sens, des organismes publics français ont déjà eu recours à des serveurs web d'entreprises étrangères tels qu'*Amazon Web Service* (AWS), *Microsoft Azure* ou encore *Google* à des fins d'hébergement de leurs données. De même, la collaboration entre la société américaine *Palentir* et les services français de sécurité intérieure (renseignements et DGSI) a fait l'objet de critiques. Voir notamment : ROSEMAIN (M.), « La DGSI renouvelle son contrat avec l'Américain Palantir, faute de système 100 % français », *op. cit.* ; RIMBOT (A.), « Hébergement de la data en France : un devoir de souveraineté numérique », *appvizer*, 20 décembre 2022 [en ligne] consulté le 21 décembre 2022.

[2254] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, pp. 111-112 : « Si la règle générale doit rester celle de fournir aux services de sécurité les meilleures technologies disponibles, indépendamment de leur nationalité, une solution nationale pourrait être privilégiée pour […] la protection des données sensibles pour l'État et pour les citoyens français [et] pour l'autonomie des forces de sécurité en cas de défaillance d'un fournisseur étranger ».

France ou au sein de l'UE des centres d'hébergement des données (*datacenters*) traitées par l'État est une solution indispensable en vue de prévenir les atteintes portées à leur confidentialité ou encore à leur disponibilité. Cette garantie suppose également que la gestion de ces centres d'hébergement des données soit assurée par des entreprises nationales ou, *a minima*, par des entreprises européennes qui sont soumises au respect des règles issues du droit européen.

775. Aujourd'hui, ces enjeux sont davantage pris en considération au regard de la demande croissante de centres d'hébergement des données localisés en Europe[2255]. La coopération entre OVHcloud et T-Systems (Deutsche Telecom) sur le projet Gaia-X a pour objectif de développer une offre de *cloud* public de confiance pour l'Allemagne, la France et d'autres marchés européens[2256] mais l'intégration d'acteurs étrangers au sein du projet pourrait avoir compromis les intentions initiales…[2257] Toutefois, un autre projet européen, baptisé « Next Generation Cloud Infrastructure and Services » et validé par la Commission européenne, pourrait répondre aux besoins d'un *cloud* européen[2258].

776. Enfin, les contrats de commande publique relatifs aux SIA devront respecter certaines exigences. Les technologies de surveillance « augmentées » de sécurité publique étant en mesure de collecter des DACP, notamment des données sensibles, il apparait opportun de limiter les possibilités d'acquisition de ces technologies auprès des entreprises soumises aux droits de l'Union européenne afin d'assurer une pleine maitrise des données (données d'apprentissage et données d'usage). Les conditions permettant de déterminer si un SIA est soumis au droit européen sont indirectement précisées par l'article 2 du REIA qui définit son champ d'application[2259]. Aussi, le Conseil d'État recommandait d'introduire dans les contrats relatifs à l'acquisition de SIA des clauses précisant les possibilités de réutilisation des données par le prestataire, le contrôle de

---

[2255] Voir en ce sens : ROCHEFORT (M.), « La demande en datacenters boostée par la souveraineté des données », *Siècle Digital*, 4 août 2023 [en ligne] consulté le 4 août 2023.

[2256] GAIA-X [en ligne]. Voir sur le sujet : TREILLES (C.), « Gaia-X : Le hub français invite les volontaires à rejoindre ses rangs », *zdnet.fr*, 25 janvier 2021 [en ligne] consulté le 28 janvier 2021.

[2257] Voir en ce sens : GAVOIS (S.), "Gaia-X « vit toujours » et « arrive à des étapes très concrètes » », *Next Ink*, 4 décembre 2023 [en ligne] consulté le 7 décembre 2023.

[2258] « Cloud : 1,2 milliard d'euros pour un Projet important d'intérêt européen commun », *Next Ink*, 8 décembre 2023 [en ligne] consulté le 8 décembre 2023.

[2259] REIA, art. 2 §1 : Un SIA sera soumis aux exigences du droit européen dès lors qu'il est mis sur le marché ou utilisé au sein de l'UE (que le fournisseur soit établi dans l'UE ou non) ou si le fournisseur et l'utilisateur sont établis hors de l'UE mais que les résultats du SIA sont exploités sur le territoire de l'UE.

l'administration sur l'usage et le transfert des données ainsi que les mesures garantissant leur destruction post-mission[2260].

777. À l'heure où les technologies, potentiellement « augmentées », occupent une place prépondérante dans les activités des forces de sécurité publique, le Général d'armée Watin-Augouard était parvenu à la conclusion que « le partenariat public-privé [était] une nécessité » mais ajoutait cependant que « seul l'État [pouvait] l'organiser »[2261]. De fait, il semble évident que les outils numériques employés par l'État n'ont fait qu'amplifier les besoins de recourir à des contrats de partenariat avec le secteur privé. Néanmoins, l'État a le devoir d'assurer la maitrise de ce partenariat en vue d'assurer sa souveraineté. Ainsi qu'il a été démontré précédemment, le maintien de la souveraineté de l'État sur ses outils et sur les données dont il assure le traitement constitue une garantie de protection des droits et libertés.

§2. Les mesures pour garantir un usage des technologies de surveillance « augmentées » de sécurité publique respectueux des droits et libertés

778. La garantie du respect des droits et libertés quant à l'usage de technologies de surveillance « augmentées » de sécurité publique ne peut être assurée que dans la mesure où les agents conservent leur pouvoir décisionnel et disposent des compétences afin d'en maitriser le fonctionnement (A). Aussi, face aux nombreux enjeux que présentent les menaces portées aux SI, la protection des droits et libertés nécessite la mise en œuvre de mesures juridiques, techniques et organisationnelles de sécurisation des technologies à l'usage de la sécurité publique dès la conception et tout au long de leur cycle de vie (B).

A. Les conditions d'utilisation assurant une « maitrise » des technologies de surveillance « augmentées » de sécurité publique

779. Les technologies de surveillance « augmentée » de sécurité publique ne peuvent reposer que sur une aide à la prise de décision afin de garantir que les forces de l'ordre conserveront leur pouvoir décisionnel (1). Or, la maitrise de ces technologies nécessite l'acquisition et le

[2260] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 133.

[2261] WATIN-AUGOUARD (M.), « La cybersécurité, enjeu de la souveraineté à l'ère numérique », *Dalloz IP/IT* n° 3, 22 mars 2021, p. 130.

renouvellement des compétences des agents qui en auront l'usage ainsi qu'un renforcement des ressources humaines du ministère de l'Intérieur (2).

1. Un nécessaire maintien du contrôle humain des décisions prises à l'aide d'une technologie de surveillance « augmentée » de sécurité publique

780. Les progrès observés concernant les SIA ont pu donner l'illusion qu'ils étaient en mesure de se substituer aux humains en produisant des résultats plus objectifs, rapides et rationnels, parfois en dépit d'une certaine opacité[2262]. Cette technologie s'est ainsi progressivement imposée comme une solution nécessaire à l'amélioration de l'exécution des missions de sécurité publique telle qu'en atteste l'adoption de la loi JOP2024 relative à l'expérimentation de la vidéoprotection « augmentée ». Les SIA peuvent être soumis à différents degrés d'automatisation des tâches : partielle, conditionnelle ou encore supervisée[2263]. Dans le cadre des technologies de surveillance « augmentées » de sécurité publique, les résultats des SIA devront soit faire l'objet d'une validation systématique par les agents préalablement à la prise de décision soit pouvoir être ignorés[2264].

781. Afin de prévenir les décisions arbitraires prises sur le fondement d'un SIA à haut risque, tels que ceux à l'usage des forces de l'ordre, le législateur européen impose que la décision finale revienne à l'humain[2265]. La soumission au contrôle humain des SIA à haut risque repose sur un objectif de prévention ou *a minima* de réduction des atteintes portées aux droits et libertés qui résulteraient d'un usage inadapté ou d'erreurs du SIA. Ce contrôle suppose que l'agent ayant recours à un SAAD dispose des compétences pour comprendre son fonctionnement, soit en mesure d'interpréter ses résultats, de détecter les anomalies et d'interrompre son usage s'il estime que le dispositif ne remplit pas correctement les finalités pour lesquelles il est utilisé[2266]. Néanmoins, ce principe ne permet pas de prévenir l'influence de l'usage d'un SAAD sur la prise de décisions des

---

2262 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 254. Voir aussi : LAZARO (C.), « Le pouvoir "divinatoire" des algorithmes : de la prédiction à la préemption du futur », *Anthropologie et Sociétés*, Vol. 42, n°2-3, 2018, pp. 127-150 [en ligne].

2263 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 102-103.

2264 Pour rappel, la règlementation en matière de protection des DACP interdit la prise de décision entièrement automatisée en matière de sécurité publique (DPJ, art. 11 ; LIL, art. 95).

2265 REIA, art. 14.

2266 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 102.

agents de sécurité publique[2267]. De fait, le recours à des SIA est susceptible d'engendrer deux types de biais influençant les utilisateurs dans leur prise de décision : le biais d'ancrage et le biais d'automatisation[2268]. Le biais d'ancrage repose sur la difficulté pour un agent de se « libérer » de la première impression laissée par le résultat produit par le SIA concernant l'analyse d'un évènement particulier. Le biais d'automatisation, comme son nom l'indique, décrit la tendance des utilisateurs à faire davantage confiance aux résultats produits par le SIA afin de rendre leurs décisions plutôt qu'à leur propre raisonnement[2269]. Aussi, le REIA exige des concepteurs des SIA à haut risque de mettre en œuvre des mesures afin de prévenir ce type de biais[2270].

782. Outre l'influence que peuvent avoir les SIA sur les décisions des agents, le recours à des technologies de sécurité publique ne doit pas entraver l'exercice de leurs missions. Dès lors, il convient de mettre en œuvre un plan de continuité des activités qui en cas de défaillance du SIA, à court terme ou à long terme, permettra aux agents d'assurer leurs missions. Aussi face à l'influence que peut avoir le recours à des technologies (assistanat numérique), le Conseil d'État recommandait l'adoption de mesures d'acculturation des agents aux nouveaux enjeux numériques que présentent les SIA[2271]. Pour rappel, la Loi pour une République numérique exige des acteurs publics d'assurer « l'indépendance » de leurs SI[2272], qui au sens du Conseil d'État suppose que « le logiciel choisi ne rende pas l'utilisateur dépendant de ses fonctionnalités »[2273]. Aussi, la maitrise des SIA à des fins de sécurité publique suppose que les agents qui en ont l'usage puissent toujours être mis en relation avec un interlocuteur humain qui dispose des compétences suffisantes afin de résoudre une éventuelle défaillance du système. En outre, l'introduction de technologies « augmentées » à des

---

2267 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 53 : « dans un contexte de décisions routinières, la vigilance de l'humain qui prend une décision est amoindrie et […], de fait, c'est la machine qui prend la décision ».

2268 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 104.

2269 REIA, art. 14, 4° b). L'observation de ce biais avait déjà été effectué par le Conseil d'État, dans son étude annuelle de 2014 qui s'inquiétait de la possibilité que « les systèmes présentés comme relevant de "l'aide à la prise de décision" soient en réalité presque toujours suivis et commandent la décision, l'intervention humaine n'étant alors qu'apparente ». Afin de remédier à ce biais, le Conseil d'État préconisait « d'indiquer dans un instrument de droit souple les critères d'appréciation du caractère effectif de l'intervention humaine » (CE, Étude annuelle sur « Le numérique et les droits fondamentaux », 2014, *op. cit.*).

2270 REIA, art. 14, 3°.

2271 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, spéc. p. 164.

2272 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *op. cit.*, art. 16.

2273 Sénat, Séance du 27 avril 2016 Débats portant sur le projet de loi pour une République numérique [en ligne].

fins de sécurité publique conduit à repenser les ressources dont doit disposer le ministère de l'Intérieur afin d'assurer une garantie effective des droits et libertés.

2. Un renouvellement des compétences du ministère de l'Intérieur

783. La maîtrise des technologies « augmentées » de sécurité publique ne doit pas se restreindre à la simple compréhension de son fonctionnement. L'emploi de technologies « augmentées » par les forces de sécurité publique devra par conséquent reposer sur une formation adaptée des agents[2274]. De manière similaire aux télépilotes de drones aériens qui doivent valider des épreuves théoriques et pratiques permettant le contrôle de l'aéronef, les agents qui feront usage de technologies « augmentées » devront suivre une formation leur permettant d'assurer la maitrise de l'outil algorithmique. Aussi, face aux enjeux croissants causés par les cybermenaces, une formation des agents aux mesures élémentaires de sécurité des SI s'avère indispensable dans le cadre du processus général d'utilisation[2275]. En ce sens, il était préconisé de renforcer les sujets liés au numérique dans le cursus et le plan de formation des agents des forces de l'ordre incluant une sensibilisation aux « aspects techniques, mais aussi [juridiques] et […] éthique[s] en matière de sécurité et d'emploi des technologies »[2276].

784. Ces différents aspects nécessitent un certain niveau d'expertise technique et juridique que ne peuvent posséder tous les agents. En conséquence, le ministère de l'Intérieur doit renouveler sa politique des ressources humaines afin de recruter des personnes disposant des compétences nécessaires dans le domaine informatique et juridique portant sur les questions relatives aux algorithmes « augmentés »[2277]. En ce sens, le Sénat préconisait la création d'un service au sein de l'État composé d'experts juridiques dont la mission consisterait à accompagner les forces de l'ordre

---

2274 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 163 : « Aucun SIA présentant une certaine sensibilité ne doit être déployé sans une formation spécifique des agents au SIA déployé. Une telle formation est au nombre des mesures organisationnelles que le projet de règlement européen prévoit d'imposer, de façon générique, au titre de la supervision humaine, pour les SIA à haut risque ».

2275 DOARÉ, Ronan, DANET, Didier et de BOISBOISSEL, Gérard, *Drones et killer robots : Faut-il les interdire ?*, op. cit., p. 187.

2276 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 50.

2277 Voir en ce sens : CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 166-167.

dans leurs démarches notamment auprès de la CNIL[2278]. Aussi, il était recommandé de développer les partenariats avec les chercheurs universitaires afin de faire coïncider leur approche scientifique avec les pratiques sur le terrain des forces de sécurité publique[2279]. Afin de répondre à ces besoins, l'adoption de la LOPMI du 24 janvier 2023[2280] visait notamment à allouer au ministère de l'Intérieur un montant de quinze milliards d'euros pour les cinq années à venir[2281] afin de renforcer ses moyens humains, juridiques mais aussi numériques[2282].

785. Enfin, la maitrise de ces nouveaux dispositifs de surveillance de la voie publique ne peut être pleinement assurée sans que des mesures de sécurisation soient mises en œuvre, tant par les concepteurs de ces technologies que par les agents qui en ont l'usage, afin de prévenir les menaces portées à leur encontre.

B. Les moyens de sécurisation des technologies de surveillance « augmentées » de sécurité publique

786. Loin d'être un phénomène nouveau, les atteintes portées aux outils numériques font dernièrement l'objet d'une croissance exponentielle au point de devenir une des préoccupations premières tout secteur confondu[2283]. Le rapport du *National Intelligence Council* avançait ainsi que l'augmentation des cybermenaces s'expliquait principalement par la multiplication des outils numériques[2284]. Ce début de décennie a été particulièrement marqué par l'affluence du nombre des attaques informatiques qui ont, en outre, été largement favorisées par la mise en télétravail forcée des activités durant la pandémie de COVID-19. L'accélération du nombre des attaques ayant eu lieu en 2020 n'aura épargné aucune entité, y compris les administrations et établissements publics de

---

2278 Sénat, Rapport n° 627 sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, pp. 105-106.

2279 Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », *op. cit.* ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 50.

2280 Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur (LOPMI), *op. cit.*

2281 *Idem*, art. 2.

2282 Voir notamment : WARUSFEL (B.), « La LOPMI et la transformation numérique des moyens de la sécurité intérieure », *JCP A* n° 13, 3 avril 2023, 2099.

2283 LEONETTI (X.) et FÉRAL-SCHUHL (C.), *Cybersécurité, mode d'emploi*, PUF, 2022, 372 p., p. 7.

2284 National Intelligence Council, "Structural Forces - Technology", March 2021, 65 p. p. 63 [en ligne]. Voir aussi : *Ibid* ; VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 206.

l'État[2285]. Or, l'association des missions d'intérêt général et des SI engendre d'importants enjeux en matière de cybersécurité[2286]. La multiplication des attaques informatiques met en exergue le caractère essentiel que constitue la sécurité des SI[2287]. Celle-ci prend la forme de normes générales de sécurisation des outils numériques et notamment ceux de l'État (1). Ces dispositions générales de cybersécurité s'accompagnent de recommandations s'adressant plus spécifiquement aux technologies de surveillance « augmentées » (2).

1. Les règles générales de sécurisation des technologies de sécurité publique

787. Face aux cybermenaces, les différentes institutions européennes ont entrepris de mettre en œuvre des mesures adaptées afin de lutter contre les atteintes, toujours plus virulentes, portées aux SI. La Convention de Budapest de 2001[2288] introduit pour la première fois des dispositions en matière de lutte contre la cybercriminalité en adoptant une politique pénale, une typologie des infractions portant sur les SI et les moyens à mettre en œuvre afin d'assurer l'équilibre entre les droits et libertés, d'une part, et le traitement des données, d'autre part. Par la suite, le Traité de Lisbonne de 2007[2289] a mis en œuvre un cadre de développement en matière de cyberdéfense et de cybersécurité. Toutefois, la Directive NIS 1[2290] est le premier texte, à l'initiative des institutions européennes, élaborant un ensemble de mesures unifiées visant à garantir l'intégrité des SI et des données numérisées. Face à l'ampleur et la complexité des enjeux de cybersécurité, la Commission européenne a adopté, le 28 novembre 2022, une nouvelle directive NIS 2[2291] en matière de cybersécurité qui complète et remplace la Directive NIS 1. Cette mise à jour des dispositions européennes en matière de cybersécurité vise à prendre en compte les nouvelles menaces, en

---

[2285] Sénat, Rapport d'information n° 82 sur la sécurité informatique des pouvoirs publics, *op. cit.*

[2286] DUCLERQ (J-B.), « Sécurité des systèmes d'information de l'Administration : quelles garanties pour les administrés ? », *RDP* n° 5, 1er septembre 2020, p. 1213.

[2287] LEONETTI (X.) et FÉRAL-SCHUHL (C.), *Cybersécurité, mode d'emploi*, *op. cit.*, p. 13.

[2288] Conseil de l'Europe, Convention sur la cybercriminalité, 23 novembre 2001, Budapest [en ligne].

[2289] Traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, Lisbonne (TFUE),13 décembre 2007, *JOUE* C 306 du 17 décembre 2007 [en ligne].

[2290] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite « NIS 1 », *JOUE* L 194 du 19 juillet 2016 [en ligne].

[2291] Directive (UE), 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), dite « NIS 2 », *JOUE* L 333/80 du 27 décembre 2022 [en ligne].

perpétuelle expansion, ciblant les SI et entend favoriser une meilleure cohésion entre les différents États membres. En outre, elle élargit le champ des domaines auxquels elle peut s'appliquer. La Directive NIS 2 sera prochainement transposée d'ici la fin de l'année 2024.

788. Aussi, les institutions européennes ont adopté un Règlement le 17 avril 2019 portant sur la certification de cybersécurité des TIC[2292] devenu le texte de référence dans ce domaine. Il fait office de règlement général pour la cybersécurité avec pour objectif d'être une première étape dans l'édification du marché unique européen des acteurs du numérique[2293]. Il introduit notamment trois niveaux de certification de sécurité européen des produits TIC[2294]. Par ailleurs, le Règlement « Cybersécurité » consacre un principe de « sécurité dès la conception » permettant de « garantir que des mécanismes efficaces au niveau tant du logiciel que du matériel sont incorporés de manière fiable »[2295]. En outre, il instaure également une auto-évaluation par le fabricant ou le fournisseur de la conformité des produits, services ou processus TIC[2296].

789. Enfin, d'autres initiatives devraient être prochainement mises en œuvre afin d'apporter des solutions concrètes de lutte contre les attaques informatiques. Ainsi, en avril 2023, le Commissaire européen annonçait la création d'un bouclier cyber-européen qui pourrait être opérationnel dès 2024[2297]. Il consisterait en un ensemble de centres de sécurité informatique établis dans les différents États membres afin de réagir au plus vite aux différentes attaques. En outre, il aura pour objectif de former de nouveaux acteurs de la cybersécurité encore trop peu nombreux.

790. Les institutions internationales ont également produit des sources en matière de cybersécurité, au rang desquelles le Manuel de Tallinn[2298] fait figure de premier guide de lutte

---

[2292] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 (Règlement « Cybersécurité »), *op. cit.*

[2293] CAPRIOLI (É.), « Vers un marché unique des acteurs de la cybersécurité », *op. cit.*

[2294] Règlement « Cybersécurité », art. 52.

[2295] *Idem*, cons. 87.

[2296] *Idem*, art. 53.

[2297] BASCOU (S.), « Cyberattaques : en quoi consiste le « bouclier cybereuropéen » voulu par l'UE ? », *01net*, 5 avril 2023 [en ligne] consulté le 1 avril 2023.

[2298] NATO, Tallin Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 215 p. [en ligne].

contre les cybermenaces. Il comprend des règles volontairement non contraignantes[2299] qui ont été définies par des experts mandatés par l'Organisation transatlantique nord (OTAN) en vue d'adapter certains aspects juridiques aux particularités propres au domaine numérique. Aussi, plusieurs sources normatives existent « afin de déterminer précisément les mesures de sécurité et de confidentialité à mettre en place »[2300]. Une des principales normes utilisées est la norme ISO 27001 énumérant les exigences relatives à la protection d'un système de management de l'information.

791. En France, plusieurs dispositions juridiques ont été adoptées afin d'encadrer spécifiquement l'usage des SI par le secteur public (a). En outre, l'ANSSI a mis en œuvre plusieurs guides méthodologiques en vue de prévenir les atteintes portées aux SI (b).

a. Les mesures de cybersécurité des SI publics

792. En France, les menaces pesant sur la sécurité des outils numériques de l'État font depuis longtemps l'objet de mesures techniques et juridiques. Depuis 2005, l'État tente de renforcer les moyens de lutte contre la cybercriminalité[2301]. En ce sens, une première ordonnance publiée le 8 décembre 2005 avait introduit une obligation de publication d'un référentiel général de sécurité à destination des responsables des administrations et établissements publics de l'État[2302]. En 2009, l'ANSSI devient la nouvelle autorité administrative indépendante en charge de la sécurité numérique de l'État en France[2303]. Depuis le décret du 11 février 2011[2304], l'ANSSI assure la double mission d'édicter des règles de protection des SI de l'État, d'une part, et d'en assurer le contrôle,

---

2299 EDDAZI (F.), « La cybervulnérabilité des drones militaires : enjeux du combat numérique », p. 200 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

2300 BENSOUSSAN-BRULÉ (V.) et TORRES (C.), *Failles de sécurité et violation des données personnelles*, *op. cit.*, p. 4.

2301 Voir à ce sujet : Ministère de l'Intérieure, Rapport sur « La cybercriminalité » délivré par BRETON (T.), 1er février 2005, 22 p. [en ligne].

2302 Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, *JORF* n°286 du 9 décembre 2005, art. 9 [en ligne].

2303 Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », *JORF* n°0156 du 8 juillet 2009, art. 1er et 2 [en ligne].

2304 Décret n° 2011-170 du 11 février 2011 modifiant le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », *JORF* n°0037 du 13 février 2011 [en ligne].

d'autre part[2305]. Aussi, elle est en charge de la sécurité des OIV qui font, en outre, l'objet de plusieurs dispositions en vue d'assurer leur intégrité[2306].

793. À partir de 2014, l'ANSSI met en œuvre un cadre de gouvernance de la sécurité numérique de l'État et publie une Politique de sécurité des systèmes d'information de l'État[2307] (PSSIE) qui s'applique à chaque ministère et consacre les règles de protection des SI de l'État. En outre, elle introduit dix principes fondamentaux portant sur la conception des SI, la gouvernance de la sécurité ainsi que les mesures en matière de sensibilisation des acteurs[2308]. Elle encourage les administrations à ne recourir qu'à des produits et services certifiés par elle ainsi qu'à privilégier un hébergement des données sur le territoire national.

794. Le décret n° 2019-1088 du 25 octobre 2019[2309] a permis de définir les systèmes d'information et de communication de l'État et introduit de nouvelles responsabilités de sécurité des SI à l'égard du Premier ministre. Ce décret a récemment été modifié par le décret n° 2022-513 du 8 avril 2022[2310] qui consacre des règles de gouvernance de la sécurité au sein des administrations de l'État. Le texte introduit une procédure d'homologation de sécurité des produits et services numériques de l'État qui devient obligatoire pour tous les SI de l'État. Il renforce les compétences du Premier ministre en matière de sécurité des SI de l'État et étend les obligations des différents ministres en matière d'organisation de la sécurité. En outre, il introduit l'obligation pour chaque ministère de désigner une ou plusieurs autorités qualifiées en matière de sécurité des SI (AQSSI) qui auront pour mission d'identifier les risques pesant sur les SI de l'État (non classifiés) et de

---

2305 VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 212.

2306 Les opérateurs d'importance vitale font l'objet d'une protection particulière en matière de cybersécurité par une première loi n°2005-1550 du 12 décembre 2005, *op. cit.* (intégrée dans le code de la défense), et plus récemment par la loi de programmation militaire du 13 juillet 2018, *JORF* n°0161 du 14 juillet 2018 [en ligne] ayant par la suite fait l'objet du décret 2018-1136 du 13 décembre 2018, *JORF* n°0289 du 14 décembre 2018 [en ligne]. La Directive (UE) 2016/1148 « Network Information Security System » (NIS) du 6 juillet 2016, *op. cit.*, et la loi de transposition (SRSI) du 26 février 2018 sur la sécurité des réseaux et systèmes d'information, *JORF* n°0048 du 27 février 2018 [en ligne] comprennent également des dispositions portant sur la cybersécurité des systèmes d'information des opérateurs d'importance vitale.

2307 ANSSI, Politique de sécurité des systèmes d'information de l'État, (PSSIE) 17 juillet 2014, 42 p. [en ligne].

2308 MATTATIA (F.), « Gouvernance de la sécurité numérique des administrations », *JCP A* n° 23, 13 juin 2022, act. 394.

2309 Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique, *op. cit.*

2310 Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics, *JORF* n°0085 du 10 avril 2022 [en ligne].

mettre en œuvre des mesures de sécurité adaptées.

795. Enfin, la récente LOPMI du 24 janvier 2023[2311] prévoit une transformation numérique du ministère avec en projet l'attribution de nouveaux outils numériques et de crédits qui permettront de créer une école de formation en cybersécurité destinée aux agents des forces de l'ordre[2312]. Ces dispositions viennent concrétiser les besoins soulignés dans le Livre blanc de la sécurité intérieure de 2020[2313].

b. La méthodologie de prévention contre les cybermenaces

796. Les cybervulnérabilités des drones aériens « augmentés » présentent un potentiel réel d'entrave aux missions de sécurité publique et, de surcroit, d'atteintes aux droits et libertés des personnes dont les DACP sont collectées. Or, la cybervulnérabilité des technologies à l'usage de la sécurité publique est susceptible d'affecter la confiance et d'induire un rejet de celles-ci par la population[2314]. Dès lors, ces technologies doivent être soumises dès leur conception à des niveaux élevés de cybersécurité. En d'autres termes, le recours à des technologies « augmentées » de sécurité publique nécessite la mise en œuvre d'un ensemble de règles, de procédures et de mesures techniques permettant d'en assurer la maitrise et de prévenir les atteintes portées aux systèmes d'information[2315]. En ce sens, la réglementation sur la protection des DACP collectées attribue des obligations de sécurité de ces données aux responsables de traitement[2316] suivant un principe de précaution. En vertu des recommandations du CEPD, les entités étatiques traitant des DACP à des fins de prévention et de répression des infractions doivent en assurer la sécurité notamment en mettant en œuvre des mesures de prévention contre les accès non-autorisés (mesures de

---

[2311] Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, *op. cit.*

[2312] WARUSFEL (B.), « La LOPMI et la transformation numérique des moyens de la sécurité intérieure », *op. cit.* ; « La LOPMI est publiée », *Newsletter LexisNexis*, 26 janvier 2023 [en ligne].

[2313] Ministère de l'Intérieur, « Livre blanc de la sécurité intérieure », *op. cit.,* pp. 183-185 et pp. 207-210.

[2314] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 43.

[2315] Code de la cybersécurité, Livre 1er, p. 5.

[2316] RGPD, art. 5, f) et 32 ; DPJ, art. 4, f), art. 29 et cons. 28 et 71 ; LIL, art. 121.

confidentialité)[2317].

797. La mesure des besoins en matière de cybersécurité constitue une étape essentielle tant dans le processus d'élaboration des outils connectés que dans celui de leur utilisation. L'ANSSI insiste ainsi tout particulièrement sur l'importance liée à la prévention des cyberattaques (mise en œuvre de mesures organisationnelles et techniques de sécurisation des systèmes d'information, tests de robustesse de ces systèmes) et sur les besoins de renforcer les mesures permettant de réagir à une attaque (qu'elle constate, à regret, comme étant toujours trop tardive)[2318]. Dans le secteur public, certains États testent et mettent régulièrement à l'épreuve l'état de leurs systèmes de cybersécurité, afin de prévenir les cyberattaques et maintenir un niveau de sécurité optimal de leurs SI. Ces tests se doublent généralement d'une recherche approfondie des différentes attaques ayant pu être recensées à l'encontre d'autres agences gouvernementales à l'instar de l'opération 'Synthetic Theology' menée en 2018 par l'*US Cyber Command* dont l'objectif consistait à sonder les réseaux d'autres pays afin d'obtenir des renseignements sur les menaces[2319].

798. Ainsi, l'anticipation des différents types d'attaques informatiques se situe au cœur de la cybersécurité. Aujourd'hui, celle-ci repose encore majoritairement sur la résolution des conséquences liées aux attaques plus qu'à leur anticipation. Une part de la méthodologie de défense face aux cybermenaces consiste à définir et à identifier les différents types de menaces pouvant potentiellement porter atteinte aux SI. L'anticipation des failles de sécurité est assurée par une équipe associant le responsable de la sécurité informatique (RSSI) et le DPD. Elle repose notamment sur la mise en œuvre d'une procédure de support à l'équipe de gestion des failles de sécurité[2320]. Si une faille de sécurité venait à être détectée, l'autorité publique, en tant que responsable de traitement des DACP collectées, devrait créer une cellule de crise constituée

---

[2317] EDPB, Recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, 2 février 2021, v. 1, 19 p., p. 14, h) §46 [en ligne] : Le principe de sécurité et de confidentialité des DACP inclus « la protection contre le traitement illicite, et les mesures appropriées pour y répondre, et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ».

[2318] GUINIER (D.), « Sécurité : Vulnérabilité aux cyberattaques du GPS à usage civil », *op. cit.* : Il est crucial d'effectuer préalablement à toute utilisation une « veille active autant sur les vulnérabilités des nouveaux composants que sur les menaces naissantes pour s'assurer des mesures les plus appropriées à la réduction du risque et à l'amélioration de la sécurité ».

[2319] NAKASHIMA (E.), "At nations' request, US Cyber Command probes foreign networks to hunt election security threats", *Washington Post*, May 7th 2019 [en ligne].

[2320] BENSOUSSAN-BRULÉ (V.) et TORRES (C.), *Failles de sécurité et violation des données personnelles*, *op. cit.*, p. 58.

d'agents exerçant différentes compétences afin de mettre en œuvre une stratégie de résolution de crise. La constitution de cette cellule de crise a pour mission de déterminer et d'approuver les mesures techniques et juridiques à mettre en œuvre. Dès lors, le travail des chercheurs en informatique tout comme celui des RSSI est capital dans la mesure où il permet d'éprouver la résistance des SI en identifiant les failles et les menaces potentielles[2321] ainsi qu'à anticiper les menaces par la mise en œuvre de mesures organisationnelles et techniques de défense.

799. Aux fins d'aider à la mise en œuvre des mesures de cybersécurité, l'ANSSI et la CNIL assurent un accompagnement des différents acteurs en publiant plusieurs guides et référentiels[2322]. L'ANSSI a récemment révisé sa méthode EBIOS[2323] qui datait de 2010. Au vu notamment des évolutions fulgurantes des menaces et des méthodes d'attaques, sa méthodologie de sécurité des systèmes d'information (SI) était devenue obsolète, celle-ci ne permettant plus de prendre en compte les nouveaux scénarios d'attaques ni d'assurer la robustesse des SI face à une complexification des risques de failles de sécurité[2324]. Le 26 juillet 2022, l'ANSSI a publié une nouvelle méthode intitulée EBIOS Risk Manager[2325], qui révise son approche des risques liés au numérique et entend être à la fois plus effective et exhaustive que la précédente face aux difficultés auxquelles sont quotidiennement confrontés les RSSI. En outre, l'Agence française de normalisation a publié un référentiel de bonnes pratiques visant à prévenir et à gérer la fuite d'informations[2326]. Elle propose ainsi de séparer les compétences de la cellule de crise en une cellule qui prendrait en charge les aspects décisionnels et une autre qui s'occuperait des aspects opérationnels.

[2321] Il s'agit d'une technique appelée *pentesting* en termes anglo-saxons où les attaquants (*hackers*) cherchent à pénétrer dans le SI et à éprouver sa résistance aux attaques.

[2322] Le site de l'ANSSI dispose d'une rubrique « Bonnes pratiques » comprenant un ensemble de guides et recommandations en matière de sécurité des SI [en ligne]. Le 17 mai 2023, l'ANSSI a publié un nouveau guide sur « Les mesures cyber préventives prioritaires », 3 mai 2023 [en ligne]. La CNIL dispose elle aussi d'un « Guide de la sécurité des données personnelles » dont la dernière version date du 3 avril 2023 [en ligne].

[2323] ANSSI, « Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) : Méthode de gestion des risques », 25 janvier 2010 [en ligne].

[2324] ANSSI, « Management du risque : obsolescence de la méthode EBIOS 2010 », 26 juillet 2022 [en ligne] consulté le 26 juillet 2022.

[2325] ANSSI, « EBIOS Risk Manager (EBIOS RM) : Méthode d'appréciation et de traitement des risques numériques », 26 juillet 2022 [en ligne].

[2326] AFNOR, Guide AFNOR BP Z90-001 « Prévention et gestion de la fuite d'information : Référentiel de bonnes pratiques », décembre 2014 [en ligne] consulté le 19 août 2017.

800. Ces règles communes applicables à tous les SI se complètent de mesures dédiées expressément à l'emploi de technologies de surveillance « augmentées » permettant de réduire leurs potentialités d'atteinte et ainsi de renforcer les garanties protégeant les droits et libertés.

2. Les recommandations spécifiques de sécurisation des technologies de surveillance « augmentées » de sécurité publique

801. Les règles générales régissant la sécurité des outils numériques sont une première étape indispensable à la sécurisation des drones aériens « augmentés » de sécurité publique. Néanmoins, face aux enjeux spécifiques que présentent la conception et l'emploi de ces technologies, les chercheurs et les institutions dédiés au domaine de la cybersécurité, ont formulé des recommandations adaptées aux systèmes de vidéoprotection (a) ainsi qu'aux SIA (b).

a. Les mesures de sécurisation des systèmes de vidéoprotection

802. Dans ses lignes directrices de 2019, le CEPD émettait plusieurs recommandations s'agissant des dispositifs vidéo et invitait les entités gestionnaires de systèmes de vidéoprotection à assurer leur protection ainsi que celle des données traitées[2327]. En premier lieu, il incitait à mettre en œuvre des mesures visant à assurer la protection de l'infrastructure du système[2328] (notamment s'agissant des caméras mobiles comme les drones aériens), du système de traitement et de transmission des données ainsi que des données traitées[2329]. En deuxième, il enjoignait les gestionnaires de ces systèmes à assurer un contrôle strict de l'accès aux données[2330] afin d'assurer le principe de confidentialité.

803. Dans le même sens, l'ANSSI a publié des recommandations de sécurité spécifiques à l'installation et à l'usage des technologies de vidéoprotection. Elle publia une première version du guide de recommandations en matière de vidéoprotection le 14 février 2013[2331]. Aujourd'hui, au vu

---

[2327] EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », *op. cit*., pp. 33-34 §§ 132-135.

[2328] *Idem*, § 133 : Intégrité ou sécurité physique du système.

[2329] *Idem*, § 134.

[2330] *Idem*, § 135.

[2331] ANSSI, « Recommandations de sécurité n°524/ANSSI/SDE pour la mise en oeuvre de dispositifs de vidéoprotection », 14 février 2013 [en ligne].

des progrès fulgurants dans ce domaine, l'ANSSI a publié un nouveau guide de recommandations relatif à la sécurisation des systèmes de vidéoprotection le 4 mars 2020[2332]. Parmi ces recommandations l'ANSSI prévoit un ensemble de mesures et de principes d'architecture informatique permettant de prévenir les vulnérabilités potentielles ou d'en limiter l'incidence[2333]. Outre les recommandations générales d'identification des acteurs, de journalisation et de gestion des alertes ainsi que de maintenance et d'exploitation des systèmes de vidéoprotection, l'ANSSI définit plusieurs autres recommandations. Ainsi, elle recommande un cloisonnement physique (ou à défaut logique) du réseau informatique du SI de vidéoprotection des autres composantes du SI de l'entité[2334] afin d'assurer la confidentialité et l'intégrité des données (éviter les intrusions et les éventuelles atteintes au dispositif ou à ses données). Aussi, elle enjoint de sécuriser le SI de vidéoprotection par une sécurisation de l'ensemble des éléments qui constituent ce SI[2335]. Elle recommande également de mettre en œuvre des mesures de chiffrement et d'authentification des flux des données des caméras de vidéoprotection[2336].

804. En outre, les experts en cybersécurité émettent plusieurs recommandations afin de prévenir plus efficacement les atteintes aux SI. À titre d'exemple, ils préconisent, en matière de réseau, d' « hybrider » l'architecture en nuage (*cloud*) afin d'assurer une meilleure protection. En d'autres termes, ils enjoignent les différents acteurs à « répartir les risques en faisant appel à plusieurs fournisseurs » ou encore de « mettre en œuvre une architecture hybride avec une partie dans le cloud, et une autre hébergée en interne »[2337]. Certes, les coûts liés à ces méthodes, et plus généralement de la sécurité informatique, sont élevés mais ils demeurent négligeables eu égard aux diverses conséquences, y compris économiques, que peut engendrer une atteinte au SI. Ces coûts sont un « mal » nécessaire que les entreprises privées comme les organismes étatiques devront

---

2332 ANSSI, « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - v2.0 », 4 mars 2020 [en ligne].

2333 GORRIEZ (F.), *Le droit de la cybersécurité*, *op. cit.*, p. 166.

2334 ANSSI, « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - v2.0 », *op. cit.*, [R10], p. 27.

2335 *Idem*, [R50] p. 59

2336 *Idem*, [R43] pp. 56-57.

2337 BISEUL (X.), « Comment se prémunir contre les attaques d'objets connectés « zombies » », *op. cit.*

accepter afin d'assurer la sécurité des données traitées. Aussi, il convient de ne pas négliger la sécurisation des structures d'hébergement des données traitées à des fins de sécurité publique[2338].

805. Enfin, les drones aériens « augmentés » de sécurité publique nécessitent la mise en œuvre de mesures protégeant la transmission des flux de données à des fins de navigabilité ainsi que ceux à des fins de surveillance. Ces besoins peuvent être assurés par la systématisation du chiffrement de bout en bout du flux des données. À titre préventif, il conviendrait également de sécuriser ses capteurs (charges utiles) des dispositifs de chiffrement ainsi que les codes sources de leur programmation face aux potentielles reconfigurations de programmation lors d'une usurpation de contrôle d'un drone aérien. Indépendamment de l'outil de vidéoprotection, l'introduction des SIA à des fins d'analyse des images issues de ces caméras suppose l'adoption de nouvelles mesures de sécurisation pour faire face aux vulnérabilités dont ils font spécifiquement l'objet.

b. Les mesures de sécurisation des SIA

806. La mise en œuvre de mesures élémentaires de sécurité des SI constitue un gage de sécurisation des systèmes et des données des drones aériens « augmentés » de sécurité publique. Cependant, les SIA sont sujets à des menaces inédites qui conduisent à mettre en œuvre des mesures spécifiques de sécurité tout au long de leur cycle de vie afin de réduire au mieux les potentialités d'atteintes à la vie privée ainsi qu'aux DACP des personnes concernées[2339]. Face à ces enjeux, le REIA enjoint les différents acteurs de recourir à des solutions techniques « adaptées aux circonstances pertinentes et aux risques »[2340] en conformité avec les analyses issues du système de gestion des risques que doivent mettre en œuvre les concepteurs. La mise en œuvre de mesures de cybersécurité des SIA constitue ainsi un pilier de la mise en conformité des technologies « augmentées » et nécessitera le recours « à des simulations d'attaque et/ou à des vérifications mathématiques pour éprouver la résistance et évaluer les vulnérabilités du système »[2341].

2338 Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 69.

2339 LINC, Dossier « Sécurité des systèmes d'IA », *op. cit.*, p. 30. Voir aussi : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 390 ; REIA, cons. 51

2340 REIA, art. 15.

2341 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 127.

807. En dépit de la complexité que revêt la sécurisation des SIA, plusieurs publications en la matière permettent de formuler cinq mécanismes préventifs de défense qui reposent sur la fiabilisation, la mise en œuvre d'un plan de déploiement, des mesures de précaution des ressources utilisées, la sécurisation du processus d'apprentissage ainsi que la mise en œuvre d'une stratégie organisationnelle[2342].

808. Le premier mécanisme préventif permettant d'assurer la fiabilité du SIA consiste à procéder à une analyse des risques spécifiques qui peuvent le menacer. Outre les mesures classiques telles qu'une étude d'impact sur les DACP, il s'agit de contrôler le processus d'alimentation du SIA (en entrée) et de maîtriser ses résultats (en sortie). De manière concrète, il est fortement recommandé d'avoir recours à des experts en sécurité informatique qui pourront effectuer des tests de mise à l'épreuve du SIA tels que des tests de pénétration du SIA (*pentesting*) ou encore de simuler une attaque informatique. Ces mesures permettent de garantir la fiabilité et la robustesse du SIA.

809. La deuxième solution de sécurité des SIA repose sur la mise en œuvre d'un plan de déploiement. En d'autres termes, il s'agit d'identifier dès la conception les exigences auxquelles le SIA devra répondre. Ces exigences incluent, dans un premier temps, l'élaboration de l'architecture du SIA en fonction des finalités envisagées qui permettra d'effectuer, dans un deuxième temps, le classement des données utilisées lors de la phase d'apprentissage afin de ne sélectionner que les données strictement nécessaires à la phase de production en application du principe de minimisation des DACP[2343]. Enfin, cette solution inclut la mise en œuvre d'une approche respectant le droit à la vie privée et la protection des DACP dès la conception (ex. mesures de chiffrement, méthodes d'anonymisation, etc.).

810. Aussi, les concepteurs de SIA doivent faire preuve de vigilance lorsqu'ils ont recours à des ressources externes (données, modèles et code). Tout d'abord, ils doivent s'assurer qu'ils exploitent légalement des données ; en d'autres termes qu'elles sont libres de droits et respectent les droits des personnes concernées (ex. droit à l'image). En outre, ces données devront répondre à des exigences de qualité (adéquation aux finalités, représentativité, correction des biais, etc.). Dans le cas de données réutilisées, un devoir de vigilance s'impose afin de garantir que ces données n'ont

[2342] LINC, Dossier « Sécurité des systèmes d'IA », *op. cit.*, pp. 30-40.

[2343] DPJ, art. 4 c) et RGPD, art. 5 c).

pas été infectées. Dans le même sens, les concepteurs devront s'assurer de la traçabilité des données[2344] qui répondent tant aux exigences juridiques qu'au niveau de performance envisagé[2345]. Enfin, la conception d'un SIA repose fréquemment sur des modèles et un code préexistants[2346]. Dès lors, les concepteurs devront s'assurer de la fiabilité de leur provenance, de leur constitution et de la mise à jour de ceux-ci précédemment à toute intégration au SIA.

811. Enfin, les deux autres mécanismes préventifs de sécurisation des SIA consistent à sécuriser la phase d'apprentissage (données et méthodes d'apprentissage) et à mettre en œuvre des mesures organisationnelles spécifiques aux SIA identifiant les choix de conception, les acteurs impliqués (phase de conception et phase d'utilisation), les stratégies de gestion des risques prévues.

812. Face à la multiplication des menaces portant sur les SI, il s'avère de plus en plus complexe d'anticiper les attaques. Paradoxalement, les SIA peuvent se présenter comme des cibles potentielles d'attaques informatiques et être également des acteurs de la cybersécurité[2347]. Dès lors, les technologies « augmentées » sont autant des atouts à l'usage de la sécurité publique que des facteurs susceptibles de nuire à son action. Les mesures de cybersécurité constituent une part cruciale des activités de sécurité publique et sont un des moteurs du renforcement de la protection des droits et libertés des personnes à l'ère des drones aériens « augmentés ».

813. Aussi, le constat des nombreuses potentialités d'atteintes aux droits et libertés que comportent les drones aériens « augmentés » de sécurité publique témoigne de la nécessité d'assurer une proportionnalité stricte de leur usage par les forces de l'ordre.

[2344] Récemment, de premières recherches ont été publiées sur les technologies déployées en vue d'opérer une traçabilité des données, voir notamment : SABLAYROLLES (A.) *et al.*, "Radioactive data: tracing through training", February 3rd 2020 [en ligne].

[2345] Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 68.

[2346] LINC, Dossier « Sécurité des systèmes d'IA », *op. cit.*, p. 34.

[2347] Les SIA peuvent participer à la détection et à la défense contre les cyberattaques (TADDEO (M.) et FLORIDI (L.), "Regulate artificiel intelligence to avert cyber arms race", *Nature*, vol. 29 (3), 2018, pp. 296-298). Voir aussi : VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, *op. cit.*, p. 214 ; « L'intelligence artificielle au service de la cybersécurité », *IA Data Analytics*, 23 janvier 2020 [en ligne] ; « Comment l'IA va bouleverser la cybersécurité ? », *Le Big Data*, 30 mai 2023 [en ligne] consultés le 30 mai 2023.

CHAPITRE 2 UN RENFORCEMENT DES GARANTIES POUR REDÉFINIR LE RAPPORT SÛRETÉ-SÉCURITÉ

814. Face aux exigences de l'ordre public, les politiques tendent souvent à adopter une position sécuritaire afin de garantir une meilleure efficacité des forces de sécurité publique. Cependant, le recours à des dispositifs de sécurité publique s'accompagne inévitablement de restrictions des droits et libertés garanties. La tendance législative accordant toujours davantage de prérogatives aux forces de l'ordre, notamment en matière d'usage d'outils numériques de sécurité publique, constitue une réelle menace pour les droits et libertés.

815. Le recours aux technologies de surveillance « augmentées » de sécurité publique vient ainsi accroitre les inégalités entre les détenteurs de la puissance publique et les personnes concernées par le traitement de DACP. L'analyse des images effectuée par les SIA de sécurité publique tend à amplifier les restrictions portées aux droits et libertés en complexifiant les possibilités pour les personnes concernées par ces traitements de faire appliquer leurs droits. En ce sens, l'opacité actuelle du fonctionnement et des usages de la vidéoprotection « augmentée », et plus particulièrement des drones aériens « augmentés » du fait de leur possible discrétion, ne permet pas aux personnes concernées d'être informées de manière effective de l'existence et des modalités de l'analyse dont elles font l'objet. De fait, au vu des analyses précédemment exposées, il apparait que le droit à l'information des personnes concernées par les traitements effectués par ces technologies ne suffit plus à assurer la protection de leurs droits et libertés. En outre, l'insuffisante fiabilité et les menaces qui pèsent sur ces technologies pourraient décupler les potentialités d'atteintes à la sûreté des personnes en restreignant les garanties inhérentes au procès pénal.

816. Néanmoins, il existe un moyen de consolider les garanties des droits et libertés au travers du principe de proportionnalité. Les mesures de police sont, en effet, soumises au respect des exigences de proportionnalité qui permettent de limiter les restrictions qu'elles exercent sur les droits et libertés. La proportionnalité repose sur l'idée d'un équilibre ou d'une conciliation dans le rapport entre l'ensemble des intérêts en présence[2348]. D'une manière générale, le principe de proportionnalité peut être défini comme « l'exigence d'un rapport, d'une adéquation, entre les

[2348] PHILIPPE (X.), *Le contrôle de proportionnalité dans les jurisprudences constitutionnelle et administrative*, éditions Economica, PUAM, coll. Sciences et droit administratif, Thèse, 1990, 499 p., pp. 19 et suiv.

moyens policiers employés et le but qui leur est assigné »[2349]. En termes juridiques, la proportionnalité est une technique juridictionnelle de « protection des droits fondamentaux à travers la modération des atteintes que pourrait leur porter la puissance publique dans la poursuite de tel ou tel but d'intérêt général »[2350]. Ainsi, le principe de proportionnalité se présente comme une solution salutaire en vue de concilier les exigences d'ordre public, qui s'expriment notamment au travers de l'usage des drones aériens « augmentés » de sécurité publique, et les droits et libertés (**Section 1**).

817. Dès lors, le contrôle de proportionnalité des restrictions à l'exercice des droits et libertés résultant des technologies de surveillance « augmentées » de sécurité publique s'avère plus que jamais nécessaire au regard des enjeux qu'elles présentent. Néanmoins, seule l'effectivité de ce contrôle permet de garantir le maintien des droits et libertés. Or, il semblerait que le contrôle de proportionnalité des dispositifs policiers de sécurité publique se révèle complexe à mettre en œuvre[2351] et nécessite de repenser la notion de proportionnalité par une meilleure prise de conscience des enjeux par les différents acteurs (**Section 2**).

Section 1 La pertinence du recours au principe de proportionnalité pour encadrer l'usage des technologies de surveillance « augmentées » de sécurité publique

818. L'origine de la notion de proportionnalité remonte à l'Antiquité grecque où Aristote employait le terme de « juste » au sein de la sphère publique comme étant « un milieu entre deux extrêmes qui, sans cela ne seraient plus en proportion ; car la proportion est un milieu, et le juste une proportion »[2352]. La proportionnalité serait donc un « mécanisme de pondération entre des principes juridiques de rang équivalent, simultanément applicables mais antinomiques »[2353]. La proportionnalité permet ainsi d'opérer une conciliation notamment entre les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, d'une

---

[2349] BRAIBANT (G.), « Le principe de proportionnalité », *in Mélanges offerts à Marcel WALINE, Le juge et le droit public*, Paris, LGDJ, Tome II, 1974, 858 p., p. 298.

[2350] XYNOPOULOS (G.), « Proportionnalité », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, spéc. p. 1251.

[2351] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 290 ; ROUSSEAU (D.), « Chronique de jurisprudence constitutionnelle 1993-1994 », *RDP* 1995, pp. 51-104, spéc. p. 73.

[2352] ARISTOTE, *Éthique de Nicomaque*, Flammarion, 1992, V, chap. 3, pp. 142-143.

[2353] XYNOPOULOS (G.), « Proportionnalité », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, spéc. p. 1251.

part, et l'exercice des droits et libertés garantis, d'autre part[2354]. Dès lors, toute mesure menant à une restriction des droits et des libertés, telle qu'une mesure de police, doit être soumise à un contrôle de proportionnalité.

819. Bien que le principe de proportionnalité ne soit pas formellement inscrit dans la Constitution française ni dans bon nombre de Constitutions étrangères[2355], celui-ci est reconnu dans la quasi-totalité des États membres de l'UE[2356]. Ce principe aurait été consacré pour la première fois par la jurisprudence allemande dans l'arrêt *Kreuzberg* de la Cour administrative suprême de Prusse du 14 juin 1882[2357]. Aujourd'hui, le principe de proportionnalité s'inspire des dispositions de « la Loi fondamentale allemande de 1949 qui garantissent une protection des droits fondamentaux[2358], d'une part, et la défense de l'État de droit[2359], de l'autre »[2360]. Cependant, il existe une différence sensible dans l'application du principe de proportionnalité. Dans sa conception « mondialisée », le contrôle de proportionnalité évalue la relation d'équilibre entre le moyen (mesure restrictive) et l'objectif poursuivi (ex. ordre public) tandis qu'en Allemagne, le juge étudie « la constitutionnalité de la limitation d'un droit fondamental »[2361]. Le principe de proportionnalité s'est répandu tant au sein des juridictions européennes (§1), dont principalement la CEDH, qu'au sein des juridictions nationales, notamment à des fins de contrôle des dispositions législatives et des mesures administratives restrictives des droits et libertés consacrés par les différentes institutions (§2).

2354 GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 290.

2355 À l'exception de la Constitution grecque, depuis sa révision constitutionnelle en 2001 (art. 25, al. 1er), et de la Constitution suisse du 18 avril 1999 (art 36, al.3 et art. 5, al.2). Voir : BOUSTA (R.), « La "spécificité" du contrôle constitutionnel français de proportionnalité », *Revue internationale de droit comparé* n°4, Vol. 59, 2007. pp. 859-877 [en ligne].

2356 ZILLER (J.), « Le principe de proportionnalité », *AJDA* n° HS, 10 juin 1996, p. 85 : Le principe de proportionnalité se retrouve dans la quasi-totalité des droits des États membres de l'Union et « est le plus souvent reconnu soit de manière explicite soit, au moins, de façon implicite » ; SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *Les cahiers de Portalis* n° 5, 2018, pp. 11 et suiv.

2357 Cour administrative suprême de Prusse, 14 juin 1882, *Kreuzberg*, cité par par SCHWARZE (J.), *Droit administratif européen*, Bruylant, 2ème édition, 2009, p. 731.

2358 Loi Fondamentale pour la République fédérale d'Allemagne, art. 19.

2359 Loi Fondamentale pour la République fédérale d'Allemagne, art. 20.

2360 SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

2361 HOCHMANN (T.), « Un succès d'exportation : la conception allemande du contrôle de proportionnalité », *AJDA* n° 14, 19 avril 2021, p. 805.

§1. La consécration du principe de proportionnalité par la jurisprudence européenne pour concilier les libertés et l'ordre public

820. Le recours au principe de proportionnalité est un témoignage d'une société démocratique qui entend garantir de manière effective le respect des droits et libertés auquel certaines mesures peuvent porter atteinte. La jurisprudence européenne s'est montrée particulièrement encline à user de ce principe. Le texte de la Conv.EDH et son interprétation par la Cour de Strasbourg mettent spécialement en avant ce dispositif de contrôle des restrictions aux droits et libertés[2362]. De manière similaire, la CJUE applique le principe de proportionnalité dans le cadre de son contrôle de l'ingérence dans l'exercice d'un droit fondamental reconnu par le droit de l'Union européenne. Ainsi, le principe de proportionnalité s'est imposé au sein des juridictions européennes, qu'il s'agisse de la CEDH (A) ou de la CJUE (B).

A. L'application du principe de proportionnalité au sein de la jurisprudence européenne des droits de l'homme

821. La proportionnalité, essence du contrôle du juge européen des droits de l'homme - Au sens de la doctrine, la proportionnalité serait « la marque incontestée du contrôle exercé par le juge européen des droits de l'homme ; elle en serait l'une des règles d'or »[2363]. Si le principe de proportionnalité s'exprime dans de nombreux États européens, le juge européen des droits de l'homme semble être de longue date celui qui l'exprime le plus nettement[2364]. Pourtant, la Conv.EDH ne fait pas expressément mention du principe de proportionnalité[2365]. En revanche, plusieurs de ses dispositions font indirectement référence à ce principe. Il en va ainsi s'agissant notamment des clauses d'ordre public où le texte énonce qu'il ne peut y avoir ingérence dans l'exercice d'un droit ou de restrictions apportées à une liberté que si celles-ci constituent des « mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de

---

[2362] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

[2363] PETITTI (L.-E.), « Réflexions sur les principes et les mécanismes de la Convention. De l'idéal de 1950 à l'humble réalité d'aujourd'hui », *in* PETITTI (L.-E.), IMBERT (P.-H.) et DECAUX (E.) (dir.), *La Convention européenne des droits de l'Homme. Commentaire article par article*, Paris, Economica, 1995, 1230 p., p. 33.

[2364] FROMONT (M.), « Le principe de proportionnalité », *AJDA* n° HS, 20 juin 1995, p. 156 ; SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.* ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.*

[2365] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 299.

l'ordre, de la santé ou de la morale publiques, ou de la protection des droits et libertés d'autrui »[2366]. Ce sont précisément ces exigences qui ont mené la CEDH à exercer un contrôle de la proportionnalité des mesures restrictives des droits qui lui sont soumises[2367]. En d'autres termes, la Cour de Strasbourg, qui assure le contrôle du respect des dispositions de la Conv.EDH par les États parties, endosse le rôle de « garant des intérêts des individus face aux ingérences possibles et potentiellement arbitraires des autorités publiques »[2368].

822. D'autres normes font également indirectement référence à ce principe telles que l'article 14 de la Conv.EDH relatif au principe de non-discrimination[2369]. Aussi, la CEDH a déjà eu l'occasion d'appliquer ce principe dans des cas non spécifiquement prévus par le texte ou les protocoles dans un arrêt du 23 juillet 1968 introduisant la notion de « rapport raisonnable de proportionnalité entre les moyens et le but visé » en matière de discrimination[2370]. Depuis cette décision, toute la jurisprudence portant sur l'article 14 de la Conv.EDH intègre le principe de proportionnalité[2371]. La Cour de Strasbourg exerce donc un examen de proportionnalité dans le cadre de son contrôle du respect de la Conv.EDH par un État partie. À ce titre, elle s'assure que l'ingérence de l'État dans les droits et libertés garantis par la Conv.EDH est nécessaire dans une société démocratique[2372]. Elle procède ainsi à une « balance des intérêts »[2373] examinant la finalité et la nécessité[2374] de la mesure restrictive de droits et de libertés protégés par la Conv.EDH[2375].

[2366] Conv.EDH, art. 8 §2, 9 §2, 10 §2 et 11 §2.

[2367] FROMONT (M.), « Le principe de proportionnalité », *op. cit.*

[2368] GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.*

[2369] *Ibid*. Il en va de même pour les articles 1 à 3 du premier protocole de la Conv.EDH. Voir également : SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

[2370] CEDH, 23 juillet 1968, *Affaire relative à certains aspects du régime linguistique de l'enseignement en Belgique c. Belgique*, n° 1474/62, §§5 et 10 [en ligne].

[2371] SCHARZE (J.), *Droit administratif européen*, Bruxelles, 1995, p. 750 cité par FROMONT (M.), « Le principe de proportionnalité », *op. cit.*

[2372] ADRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, spéc. p. 280.

[2373] Expression, remplaçant le terme habituel de « proportionnalité », utilisée dans l'arrêt CEDH, 19 janvier 2021, *Lacatus c. Suisse*, n° 14065/15, §§100 et 102 [en ligne].

[2374] Selon la jurisprudence de principe de la Cour, la notion de nécessité repose sur la recherche « d'un besoin social impérieux », en d'autres termes de l'existence de « motifs pertinents et suffisants » et proportionnés aux objectifs légitimes de la mesure examinée (CEDH, 7 décembre, 1976, *Handyside c. Royaume-Uni*, n° 5493/72, §48 [en ligne] ; CEDH, 24 mars 1988, *Olsson c. Suède* n° 1, n° 10465/83, §67 [en ligne]).

[2375] SUDRE (F.), *La convention européenne des droits de l'Homme*, *op. cit.*, p. 39

823. Le contrôle de proportionnalité des mesures de sécurité publique - Le contrôle de proportionnalité des dispositifs de sécurité publique et nationale se retrouve régulièrement au sein de la jurisprudence de la CEDH[2376]. Dans l'arrêt *Lawless c. Irlande* n° 3 du 1er juillet 1961, la Cour de Strasbourg avait consacré un droit pour les États parties de « protéger la société démocratique européenne »[2377] dans les conditions spécifiques prévues par l'article 15 de la Conv.EDH qui privilégient l'exercice des libertés du collectif sur celui de chaque individu[2378]. Afin de rétablir un certain équilibre le juge avait précisé, dans sa décision *Handyside c. Royaume-Uni* du 7 décembre 1976, que « la marge nationale d'appréciation va de pair avec un contrôle européen »[2379]. En d'autres termes, la Cour de Strasbourg autorise les mesures permettant d'assurer l'exercice des libertés du plus grand nombre sur l'exercice individuel uniquement sous son contrôle. Quelques exemples de décisions de la CEDH portant sur des contrôles de proportionnalité de traitements de DACP effectués dans un cadre de sécurité publique, principalement en matière de fichiers de police, permettent d'illustrer le contrôle qu'elle exerce.

824. Dans la décision *S. et Marper c. Royaume-Uni* du 4 décembre 2008, les requérants contestaient la légalité de la conservation de leurs empreintes digitales et de leurs échantillons d'ADN au regard du droit à la vie privée protégé par l'article 8 de la Conv.EDH[2380]. Lors de son examen, la CEDH avait rappelé que « la conservation des profils ADN de personnes condamnées est autorisée, en règle générale, pendant une durée limitée après la condamnation ou après le décès du condamné »[2381]. Or, elle avait constaté que le Royaume-Uni était le seul État membre à autoriser expressément leur « conservation systématique et illimitée »[2382]. Dès lors, elle avait condamné l'État britannique pour violation du droit à la vie privée au motif que la conservation des données des requérants ne traduisait pas « un juste équilibre entre les intérêts publics et privés » et que

---

2376 À titre d'exemple : CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, *op. cit.* ; CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, *op. cit.* ; CEDH, 17 mars 2010, *B. B. c. France*, n° 5335/06 [en ligne] ; CEDH, 17 mars 2010, *Gardel c. France*, n° 16428/05 [en ligne] ; CEDH, 18 juillet 2013, *M. K. c. France*, n° 19522/09 [en ligne] ; CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.* ; CEDH, gd ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*

2377 CEDH, 1er juillet 1961, *Lawless c. Irlande* n° 3, *op. cit.*

2378 KISSANGOULA (J.), « La sécurité dans la jurisprudence de la CEDH », *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, pp. 229-252, p. 251.

2379 CEDH, 7 décembre, 1976, *Handyside c. Royaume-Uni*, *op. cit.*, §49.

2380 CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, *op. cit.*, §59.

2381 *Idem*, §48.

2382 *Ibid*.

« l'État défendeur a[vait] outrepassé toute marge d'appréciation acceptable en la matière »[2383]. Elle confirmera sa position concernant la conservation illimitée de données par les autorités publiques dans un arrêt *Catt c. Royaume-Uni* du 24 janvier 2019[2384].

825. En matière de fichiers de police, les condamnations de la France par la CEDH sont nombreuses[2385]. À titre d'exemple, l'arrêt *MK c. France* du 18 avril 2013 avait conduit le juge à sanctionner la France pour atteinte disproportionnée au droit à la vie privée au motif qu'un individu pouvait se trouver dans le fichier national automatisé des empreintes digitales pour des « infractions mineures » et que celui-ci n'effectuait aucune distinction entre les personnes ayant fait l'objet d'une condamnation et les personnes relaxées[2386]. En outre, la CEDH reprochait aux autorités françaises de n'avoir pas correctement défini la durée de conservation des DACP du fichier[2387]. Cette affaire a permis de mettre en cause un autre fichier de police (le fichier national automatisé des empreintes génétiques) dans un arrêt *Aycaguer c. France* où la CEDH a reconnu une disproportion entre la durée de conservation des données du fichier et la gravité des infractions conduisant à l'inscription[2388].

826. La CEDH a également eu à traiter d'affaires portant sur des images de systèmes de vidéoprotection ou encore de suivi de personnes tel qu'au moyen de dispositifs GPS. Dans l'affaire *Peck c. Royaume-Uni* du 28 janvier 2003, le juge européen des droits de l'homme a condamné l'État britannique pour ingérence dans la vie privée au motif que des images issues de caméras de surveillance de la voie publique permettant distinctement d'identifier la personne concernée avaient été diffusées dans les médias[2389]. L'arrêt *Uzun c. Allemagne* du 2 décembre 2010 portait sur la surveillance par GPS d'une personne suspectée de terrorisme au motif que la personne concernée faisait l'objet d'une surveillance approfondie par plusieurs autorités de l'État ce qui a permis de qualifier l'ingérence au droit à la vie privée. Ainsi, le principe de proportionnalité est

---

2383 *Idem*, §125.

2384 CEDH, 24 janvier 2019, *Catt c. Royaume-Uni*, n° 43514/15, §§127-128 [en ligne].

2385 Voir par exemple : CEDH, 18 septembre 2014, *Brunet c. France*, n° 21010/10 [en ligne] ; CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12 [en ligne].

2386 CEDH, 18 juillet 2013, *M. K. c. France*, *op. cit.*, §§41 et 42.

2387 *Idem*, §45.

2388 CEDH, 22 juin 2017, *Aycaguer c. France*, *op. cit.*, §43.

2389 CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, *op. cit.*, §62.

particulièrement présent au sein de la jurisprudence de la CEDH. Néanmoins, les dernières décisions font apparaitre une fragilité de ce contrôle.

827. La variabilité du contrôle de proportionnalité de la Cour européenne des droits de l'homme - Si le principe de proportionnalité est toujours au cœur de la jurisprudence européenne des droits de l'homme, il convient de nuancer l'importance du contrôle opéré par les juges au regard de sa variabilité, laissant une large marge nationale d'appréciation[2390]. En d'autres termes, la proportionnalité dispose toujours d'une place importante dans les décisions de la CEDH mais celle-ci tend à l'appliquer différemment et plus modérément[2391]. Le fait est que cette marge d'appréciation des États dans l'application des dispositions de la Conv.EDH constitue une auto-limitation du pouvoir de contrôle de la CEDH sur les mesures restrictives des droits et libertés mises en œuvre par les autorités nationales[2392]. Ainsi, il revient à la CEDH de déterminer le niveau d'intensité de son contrôle sur cette marge nationale d'appréciation. Or, les développements effectués précédemment démontrent, notamment s'agissant des affaires portant sur la surveillance de masse[2393] et le recours à des algorithmes de prévention des infractions[2394], qu'elle s'est montrée particulièrement souple ces dernières années (v. **n° 613 et suiv.**). De fait, la CEDH tend à privilégier le contexte de la lutte-antiterroriste pour justifier la modération de son contrôle[2395]. En ce sens, la juge Françoise Tulkens critiquait l'état actuel de la jurisprudence européenne déclarant que « consensus européen et marge d'appréciation sont de faux amis »[2396] et rappelait que les juges avaient pour devoir « d'être attentifs aux responsabilités qui sont les leurs et qui sont, en définitive,

---

2390 SUDRE (F.), *Droit européen et international des droits de l'homme*, *op. cit.*, pp. 209-210 : La marge nationale d'appréciation peut être définie comme « le rapport de compatibilité devant exister entre les mesures nationales et la norme conventionnelle ».

2391 GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.*

2392 GAUTHIER (C.), PLATON (S.) et SZYMCZAK (D.), *Droit européen des droits de l'homme*, Paris, Sirey, 2016, 518 p., p. 111.

2393 CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, *op. cit.* ; CEDH, gd ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*

2394 CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, *op. cit.*

2395 ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, *op. cit.*, p. 282 ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.* ; MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 323.

2396 TULKENS (F.), « Conclusions générales », *in* SUDRE (F.) (dir.), *Le principe de subsidiarité au sens du droit de la Convention européenne des droits de l'homme*, Bruxelles, Artemis, Némésis, 2014, 412 p., p. 403.

de véritables exigences éthiques »[2397]. Ces remarques s'avèrent tout particulièrement pertinentes à l'heure où les droits et libertés sont mis en péril par les technologies de surveillance « augmentées » de sécurité publique.

B. Le recours inégal au principe de proportionnalité par le juge de l'Union européenne

828. La CJUE recourt régulièrement au principe de proportionnalité dans le cadre de son contrôle du respect des libertés consacrées par les traités européens[2398]. Après l'avoir énoncé pour la première fois dans l'arrêt *Fédération charbonnière de Belgique* du 29 novembre 1956[2399], le juge de l'Union européenne l'a érigé au rang de principe général du droit de l'Union dans l'arrêt *Internationale Handelsgesellschaft* du 17 décembre 1970[2400]. Le principe de proportionnalité a finalement été consacré à l'article 5 §4 du Traité sur le fonctionnement de l'Union européenne[2401] (TFUE) et à l'article 52 §1 de la CDFUE[2402] afin de conditionner les limitations pouvant être portées aux droits de l'Union européenne[2403].

829. Les critères du contrôle de proportionnalité - Le principe de proportionnalité s'applique principalement en matière économique dans la jurisprudence de l'Union européenne[2404]. La CJUE, en application des dispositions du TFUE, encadre de manière stricte les limitations

---

[2397] *Idem*, p. 407.

[2398] De manière non-exhaustive : BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, pp. 240-241 ; SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.* ; CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *AJDA* n° 14, 19 avril 2021, p. 800 ; CIROTTEAU (M.), « La réception du droit de l'Union par le juge administratif en matière de conservation des données de connexion et de surveillance : la lettre plutôt que l'esprit », *JCP A* n° 50, 19 décembre 2022, étude 2345.

[2399] CJCE, 29 novembre 1956, *Fédération Charbonnière de Belgique c. Haute Autorité de la Communauté européenne du charbon et de l'acier*, aff. 8/55, § 304 [en ligne]. Puis, dans l'arrêt : CJCE, 13 juin 1958, *Compagnie des Hauts Fourneaux de Chasse c. Haute Autorité de la Communauté européenne du charbon et de l'acier*, aff. 15/57, § 192 [en ligne].

[2400] CJCE, 17 décembre 1970, *Internationale Handelsgesellschaft*, aff. 11/70, *op. cit.*, § 2.

[2401] TFUE, art. 5 §4 : « En vertu du principe de proportionnalité, le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités. Les institutions de l'Union appliquent le principe de proportionnalité conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité ».

[2402] CDFUE, art. 52 §1 : « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

[2403] CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2404] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

portées à l'exercice des libertés garanties par le droit de l'Union européenne[2405]. Aussi, le juge de l'Union européenne a souvent recours au principe de proportionnalité dans le cadre de la protection des droits fondamentaux[2406]. Ce principe s'applique tant au législateur communautaire qu'aux mesures administratives[2407]. Aux fins de contrôler la proportionnalité de l'ingérence dans l'exercice d'un droit fondamental de l'Union européenne, la CJUE applique un triple test, inspiré du modèle allemand[2408], qui repose sur trois critères : l'aptitude (ou l'adéquation), la nécessité et la proportionnalité *stricto sensu*[2409]. Aux fins d'effectuer l'examen de proportionnalité, la CJUE procède, au préalable, à une identification de l'objectif poursuivi et étudie sa légitimité[2410]. En premier lieu, le test de proportionnalité vise à déterminer si la mesure en cause est apte à atteindre l'objectif d'intérêt général poursuivi. En deuxième lieu, le juge tente de déterminer si la mesure est nécessaire à la réalisation de cet objectif. En d'autres termes, il évalue s'il n'existait pas de mesures alternatives moins restrictives en vue de le réaliser. En dernier lieu, le juge contrôle l'existence d'un juste équilibre entre les intérêts visés par cet objectif et les conséquences liées à la restriction d'un droit fondamental[2411].

830. L'intensité du contrôle de proportionnalité - Les différentes étapes du contrôle de proportionnalité sont régulièrement mentionnées dans les décisions du juge de l'Union européenne. Toutefois, l'intensité de ce contrôle varie et ne présente pas systématiquement les trois critères. Il arrive que le juge s'en tienne à une simple constatation de « la non-satisfaction de l'un des deux ou

---

[2405] Voir en ce sens : CJCE, 12 juin 2003, *Eugen Schmidberger c. Republik Österreich*, aff. C-112/00, spéc. §§ 77-82 [en ligne].

[2406] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, pp. 240-241 ; CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2407] FROMONT (M.), « Le principe de proportionnalité », *op. cit.*

[2408] GALETTA (D-U.), « Le principe de proportionnalité », *in* AUBY (J-B.) et DUTHEIL DE LA ROCHÈRE (J.) (dir), *Traité de droit administratif européen*, Bruxelles, Bruylant, 2ème édition, 2014, 1118 p., p. 501.

[2409] De manière non-exhaustive : DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, op. cit., p. 166 ; FROMONT (M.), « Le principe de proportionnalité », *op. cit.* ; CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2410] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 240 : « La Cour […] s'autorise à éventuellement qualifier l'objectif poursuivi pour souligner son importance et sa capacité à "justifier des conséquences négatives, mêmes considérables" pour les personnes concernées » ; SIMON (D.), « Le contrôle de proportionnalité exercé par la Cour de justice des Communautés européennes », *LPA*, 5 mars 2009, n° 46, p. 17. Voir notamment : CJCE, 30 juillet 1996, *Bosphorus*, aff. C-84/95, §§ 23-26 [en ligne] ; CJCE, gr. ch., 3 septembre 2008, *Kadi c. Conseil de l'Union européenne et Commission des communautés européennes*, *op. cit.*, §363 ; CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, *op. cit.*, § 42 ; CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.*, §§ 126 et suiv.

[2411] DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, op. cit., pp. 165-166 .

trois critères cumulatifs et [fasse] l'économie des autres »[2412]. Ainsi, l'intensité du contrôle de proportionnalité de la CJUE peut varier en fonction de différents facteurs tels que « l'importance de l'objectif poursuivi, la marge d'appréciation dont peu[vent] bénéficier les autorités nationales, ou encore les paramètres propres au droit en cause »[2413]. La CJUE peut ainsi effectuer un contrôle restreint ou plus approfondi ou, de manière exceptionnelle, un contrôle d'opportunité[2414]. Dernièrement, elle a ainsi exercé un contrôle étroit des mesures portant sur la conservation massive et indifférenciée de données issues des communications électroniques à des fins de lutte contre la criminalité ou de lutte contre le terrorisme[2415]. Cette position adoptée par la CJUE s'explique par l'accent mis sur la protection des droits fondamentaux, notamment du droit à la vie privée et du droit à la protection des DACP (v. **n° 624 et suiv.**). De fait, le test de proportionnalité s'est intensifié s'agissant des affaires dont les mesures en cause affectent l'exercice des droits fondamentaux.

831. L'application du contrôle de proportionnalité en matière de droits fondamentaux - L'introduction des droits fondamentaux a permis d'enrichir le contrôle de proportionnalité appliqué par la CJUE. Après avoir emprunté, dans un premier temps, la notion de « société démocratique »[2416] issue de la jurisprudence de la CEDH[2417], le principe de proportionnalité se repose pleinement sur la CDFUE pour déterminer si l'ingérence à l'un de ses droits est contraire au droit de l'Union européenne. Aussi, le lien établi entre les droits fondamentaux et le principe de proportionnalité résulte des oppositions pouvant exister entre deux droits fondamentaux. Le juge de l'Union européenne procède en ce cas à une « mise en balance des intérêts » dont la technique avait été introduite dans un arrêt *Schmidberger* du 12 juin 2003 opposant le droit à la liberté d'expression et de manifestation, d'une part, au droit à la libre circulation, d'autre part[2418].

[2412] CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2413] BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 241.

[2414] CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2415] Voir : CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, *op. cit.* ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, *op. cit.* ; CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.* ; CJUE, gr. ch., 6 octobre 2020, *Privacy International*, *op. cit.*

[2416] CJCE, 28 octobre 1975, *Rutili c. ministre de l'intérieur*, *op. cit.*, § 32 ; CJCE, 20 mai 2003, *Österreichischer Rundfunk*, *op. cit.*, §§ 76 et 82.

[2417] CEDH, 7 décembre, 1976, *Handyside c. Royaume-Uni*, *op. cit.*, § 24.

[2418] CJCE, 12 juin 2003, *Eugen Schmidberger c. Republik Österreich*, *op. cit.*, §§ 74, 77 et 81.

832. La CJUE effectue un contrôle de proportionnalité afin de concilier les impératifs de sécurité publique ou de sécurité nationale, d'une part, avec la protection des droits fondamentaux, d'autre part. Quelques décisions permettent d'illustrer le recours au contrôle de proportionnalité par le juge de l'Union européenne pour apprécier l'équilibre entre des mesures nationales de sécurité et les droits fondamentaux. La CJCE a précisé les conditions de ce contrôle en matière de lutte contre les menaces terroristes dans les arrêts *Kadi* du 3 septembre 2008[2419] et du 18 juillet 2013[2420]. Dans la première affaire, elle a indiqué que la limitation des droits fondamentaux au motif de la lutte antiterroriste n'est possible que si elle permet d'assurer l'effectivité des dispositifs techniques servant à l'objectif poursuivi[2421]. Dans la deuxième affaire, elle a estimé qu'il relevait de la compétence du juge de l'Union européenne de concilier les intérêts en matière de sécurité avec les droits fondamentaux, en l'espèce les droits de la défense[2422].

833. La doctrine a souvent critiqué le contrôle strict de proportionnalité appliqué par le juge de l'Union européenne en matière de mesures nationales[2423]. Pourtant, au regard de la jurisprudence de la CJUE, il semblerait que l'intensité du contrôle de proportionnalité puisse varier en fonction de l'objectif poursuivi. Ainsi, dans l'arrêt *Tele2 Sverige* du 21 décembre 2016 portant sur la gestion des données de connexion, la CJUE a eu recours au contrôle de proportionnalité afin de déterminer si les conséquences de l'atteinte portée aux droits fondamentaux, résultant d'une mesure de lutte contre les infractions graves, étaient équilibrées avec les apports engendrés par celle-ci[2424]. En reprenant le principe d'interdiction de la conservation généralisée et indifférenciée des données énoncées dans les arrêts précédents, la CJUE a adapté son contrôle au contexte dans l'arrêt *La Quadrature du Net*

[2419] CJCE, gr. ch., 3 septembre 2008, *Kadi c. Conseil de l'Union européenne et Commission des communautés européennes*, *op. cit.*

[2420] CJUE, gr. ch., 18 juillet 2013, *Commission européenne c. Kadi*, aff. jointes C-584/10 P, C-593/10 P et C-595/10 [en ligne].

[2421] CJCE, gr. ch., 3 septembre 2008, *Kadi c. Conseil de l'Union européenne et Commission des communautés européennes*, *op. cit.*, § 363 : « Au regard d'un objectif d'intérêt général aussi fondamental pour la communauté internationale que la lutte par tous les moyens […] contre les menaces à l'égard de la paix et de la sécurité internationales que font peser les actes de terrorisme, le gel [des] ressources économiques des personnes identifiées […] comme étant associées [à un groupe terroriste] ne saurait, en soi, passer pour inadéquat ou disproportionné ».

[2422] *Idem*, §§ 342-344 et CJUE, gr. ch., 18 juillet 2013, *Commission européenne c. Kadi*, *op. cit.*, § 125 : « Il incombe toutefois au juge de l'Union, auquel ne saurait être opposé le secret ou la confidentialité de ces informations ou éléments, de mettre en œuvre, dans le cadre du contrôle juridictionnel qu'il exerce, des techniques permettant de concilier, d'une part, les considérations légitimes de sécurité quant à la nature et aux sources de renseignements ayant été pris en considération pour l'adoption de l'acte concerné et, d'autre part, la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, tels que le droit d'être entendu ainsi que le principe du contradictoire ».

[2423] CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *op. cit.*

[2424] CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, op. cit., § 105.

et a. du 6 octobre 2020. En l'espèce, elle a estimé que la mesure très restrictive des droits et libertés était nécessaire en vue d'assurer l'efficacité de la lutte contre les infractions graves[2425].

834. Cependant, dans l'arrêt *La Quadrature du Net et a.* constitue une exception (liée aux finalités de sécurité nationale) dans la mesure où la CJUE se révèle particulièrement protectrice du droit à la protection des DACP. En ce sens, lors de son examen de la législation européenne en matière de conservation des données des clients de fournisseurs de services de communications électroniques dans l'arrêt *Digital Rights Ireland Ltd. e. a.*, la CJUE a appliqué un contrôle strict de proportionnalité conduisant à l'invalidation de la directive en cause[2426]. Dans le cadre de son contrôle, le juge de l'Union européenne a procédé à une analyse de l'adéquation des dispositions de la directive 2006/24 pour réaliser l'objectif poursuivi de lutte contre la criminalité grave[2427]. Procédant à la vérification du critère de nécessité, la CJUE a estimé que si l'objectif poursuivi revêtait « une importance primordiale pour garantir la sécurité publique et [que] son efficacité peut dépendre […] de l'utilisation des techniques modernes d'enquête »[2428] il en était de même de « la protection des données à caractère personnel [au regard du] droit au respect de la vie privée »[2429]. Ainsi, elle a considéré que cette directive ne remplissait pas le critère de nécessité. Enfin, elle a identifié trois aspects de la directive contraires au critère de proportionnalité *stricto sensu* : l'absence de distinction des métadonnées conservées entre les personnes suspectées d'être en lien avec des activités criminelles et les personnes non suspectées[2430], l'absence de critères limitant l'accès des autorités nationales aux données liées à l'objectif poursuivi[2431], et la durée excessive de conservation des données quant aux risques d'atteinte à l'ordre public[2432]. Cet arrêt témoigne de l'importance indiscutable du contrôle de proportionnalité opéré par la CJUE en matière de protection des droits et libertés, y compris s'agissant de mesures relatives à la sécurité publique ou à la sécurité nationale.

[2425] CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, *op. cit.*, § 136.

[2426] CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, *op. cit.*, § 65.

[2427] *Idem*, § 49.

[2428] *Idem*, § 51.

[2429] *Idem*, §§ 52-53.

[2430] *Idem*, §§ 57-59.

[2431] *Idem*, §§ 60-62.

[2432] *Idem*, §§ 63-64.

835. En définitive, la modulation de l'intensité du contrôle de proportionnalité de la CJUE lui permet de prendre davantage en considération les circonstances de l'espèce. Elle témoigne de l'importance du principe de proportionnalité sur le territoire de l'Union européenne appliqué aussi de longue date par les juridictions nationales.

§2. La reconnaissance du principe de proportionnalité par la jurisprudence française pour concilier les libertés et l'ordre public

836. En France, le juge administratif applique depuis longtemps le principe de proportionnalité pour contrôler les mesures prises en matière de police[2433] (A). À l'inverse, le juge judiciaire n'emploie le principe de proportionnalité que depuis peu (B). De même, le juge constitutionnel use fréquemment du contrôle de proportionnalité pour modérer l'incidence de la puissance publique sur les droits et libertés[2434] (C).

A. Le contrôle de proportionnalité des mesures de police par le juge administratif

837. La consécration du contrôle de proportionnalité - Ce principe, sans être mentionné de manière explicite[2435], était déjà évoqué par le commissaire du gouvernement Romieu en qualifiant le rôle de « tutelle contentieuse » du juge administratif sur les mesures de police dans l'arrêt *Jacquin* du 30 novembre 1906[2436]. Le rôle de contrôleur du respect du principe de proportionnalité des mesures de police par le juge administratif a été précisé dans un arrêt *abbé Olivier* du 19 février 1909[2437]. L'arrêt *Benjamin* du 19 mai 1933[2438] a permis de définitivement consacrer le pouvoir de

---

[2433] Voir notamment : DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 168 ; BRAIBANT (G.), « Le principe de proportionnalité », *in Mélanges offerts à Marcel WALINE, Le juge et le droit public*, *op. cit.*, note 5, p. 299 ; ZILLER (J.), « Le principe de proportionnalité », *op. cit.*

[2434] XYNOPOULOS (G.), « Proportionnalité », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, spéc. p. 1251.

[2435] STIRN (B.), « Ordre public et libertés publiques » *in* SÈVE (R.), *L'ordre public*, *op. cit.*, p. 11 ; SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

[2436] CE, 30 novembre 1906, *Jacquin*.

[2437] CE, 19 février 1909, *Abbé Olivier*, n° 27355, Rec. p. 181 [en ligne] : Il était demandé aux juges du Conseil d'État d'examiner « la limite des devoirs du maire et [de] rechercher si les arrêtés de police ont été pris dans l'intérêt du maintien de l'ordre public ».

[2438] CE, 19 mai 1933, n° 17413, *Benjamin*, *op. cit.*

contrôle du juge administratif[2439]. En l'espèce, le maire de Nevers avait pris la décision d'interdire une conférence controversée localement et prononcée par le sieur René Benjamin. Le Conseil d'État avait souligné que « s'il incombe au maire […] de prendre les mesures qu'exige le maintien de l'ordre, il doit concilier l'exercice de ses pouvoirs avec le respect de la liberté de réunion ». Il avait ajouté que « l'éventualité de troubles alléguée [..] ne présentait pas un degré de gravité tel qu'il n'ait pu, sans interdire la conférence, maintenir l'ordre en édictant les mesures de police qu'il lui appartenait de prendre ». Aujourd'hui, le juge administratif exerce son contrôle sur un ensemble étendu de mesures de police en s'assurant « de leur adéquation aux circonstances de temps et de lieu propres à chaque situation »[2440] dans la continuité de cette jurisprudence[2441].

838. La jurisprudence du Conseil d'État reposant sur le célèbre arrêt *Benjamin* énonce un principe de proportionnalité selon lequel les mesures de police doivent être adaptées à la situation de fait en garantissant dans le même temps le respect des droits et libertés propres à chacun. En d'autres termes, il s'assure que les autorités de police n'imposent que des mesures « strictement proportionnées »[2442] aux citoyens en effectuant une balance des intérêts entre les avantages apportés à l'ordre public et les limitations portées aux droits et libertés[2443]. Dès lors, le juge administratif a le devoir d'examiner si ces mesures sont à la fois suffisantes et non excessives. Le Conseil d'État met donc en œuvre un contrôle de proportionnalité des mesures de police qui, sans le nommer[2444], repose sur l'idée que les restrictions qu'elles apportent à l'exercice des droits et libertés en raison de motifs d'ordre public doivent être adéquates et nécessaires. Ce principe s'inscrit dans la droite

---

[2439] De manière non-exhaustive : PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 363 ; BURG (M.), *Droit fondamental et opérationnel du maintien de l'ordre public*, *op. cit.*, p. 32 ; STIRN (B.), « Ordre public et libertés publiques » *in* SÈVE (R.), *L'ordre public*, *op. cit.*, p. 11 ; ROUSSEL (S.), « Le contrôle de proportionnalité dans la jurisprudence administrative », *AJDA* n° 14, 19 avril 2021, p. 780.

[2440] STIRN (B.), « Ordre public et libertés publiques » *in* SÈVE (R.), *L'ordre public*, *op. cit.*, p. 11

[2441] Voir notamment : CE, Sect., 9 mai 1984, n° 49153 [en ligne] : « Considérant que s'il appartenait à l'autorité de police d'user à Paris des pouvoirs qu'elle tient de la loi […] pour réglementer en cas de nécessité, dans l'intérêt du bon ordre, de la tranquillité et de la sécurité publique, dans les voies et zones réservées aux piétons, les activités musicales et les attractions de toute nature, elle ne pouvait légalement […] édicter une mesure d'interdiction générale et permanente de toutes ces activités et attractions, applicable sous la seule réserve de dérogations trop limitatives, à la presque totalité des voies et zones dont il s'agit ».

[2442] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 362.

[2443] XYNOPOULOS (G.), « Proportionnalité », *in* ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, *op. cit.*, spéc. p. 1251.

[2444] ROUSSEL (S.), « Le contrôle de proportionnalité dans la jurisprudence administrative », *op. cit.*

lignée de l'arrêt *Baldy* du 10 août 1917, énonçant que « la liberté est la règle et la restriction de police, l'exception »[2445].

839. Influencé par le droit[2446] et la jurisprudence de l'Union européenne (v. **n° 828-835**), le juge administratif applique un triple test de proportionnalité reposant sur trois critères de contrôle des mesures de police qui consistent à déterminer l'adéquation, la nécessité et la proportionnalité *stricto sensu*. L'introduction du triple test de proportionnalité dans le droit français est survenue dans la jurisprudence du Conseil constitutionnel dans sa décision du 21 février 2008[2447]. Il fut consacré par la jurisprudence du Conseil d'État dans une décision d'assemblée du 26 octobre 2011 annulant pour excès de pouvoir un décret relatif aux passeports électroniques[2448]. Toutefois, l'introduction du triple test de proportionnalité au sein de la jurisprudence administrative s'avère « plus formel que substantiel »[2449] dans la mesure où le Conseil d'État opérait déjà un contrôle strict de proportionnalité des mesures attentatoires à l'exercice des droits et libertés. Tout au plus, son apparition dans les décisions du juge administratif a permis de rendre son contrôle plus explicite et précis[2450]. En outre, l'évolution de son contrôle de proportionnalité repose également sur l'introduction du référé-liberté, par la loi du 30 juin 2000[2451], qui lui permet « d'ordonner toutes mesures nécessaires à la sauvegarde d'une liberté fondamentale à laquelle […] une atteinte grave et manifestement illégale »[2452] a été portée.

840. L'application du contrôle de proportionnalité - Quelques exemples peuvent être cités en matière de contrôle des mesures de police portant sur le recours à des technologies de traitement de DACP. À cet égard, les fichiers de police ont pu parfois faire l'objet de recours devant le juge administratif. Dans un arrêt du 16 avril 2010[2453], le Conseil d'État avait été saisi d'un recours pour

---

[2445] CE, 10 août 1917, n°59855, *Baldy, op. cit.*

[2446] CDFUE, art. 52 §1.

[2447] C. const., Décision n°2008-562 DC, 21 février 2008, *op. cit.*, cons. 13.

[2448] CE, ass., 26 octobre 2011, n° 317827, *Association pour la promotion de l'image et autre* [en ligne] : Les mesures restrictives « adaptées, nécessaires et proportionnées ».

[2449] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

[2450] PETIT (J.) et FRIER (P-L.), *Droit administratif*, *op. cit.*, p. 364 ;

[2451] Loi n° 2000-597 du 30 juin 2000 relative au référé devant les juridictions administratives, *op. cit.*

[2452] CJA, art. L. 521-2.

[2453] CE, 10ème et 9ème ss-sect. réunies, 16 avril 2010, n° 320196, *Association aides et autres* [en ligne].

excès de pouvoir portant sur des décrets relatifs au traitement automatisé de DACP[2454] créant le fichier intitulé CHRISTINA[2455]. À cette occasion, le juge administratif, usant du contrôle de proportionnalité, a estimé que « le pouvoir réglementaire est autorisé à dispenser de publication certains des traitements qui intéressent la sûreté de l'État, la défense ou la sécurité publique, dès lors que les données enregistrées […] sont en adéquation avec la finalité du traitement et proportionnées à cette finalité ». En outre, il a considéré que compte tenu des finalités du traitement et de la proportionnalité de la nature des données enregistrées « le traitement automatisé dénommé CRISTINA ne porte pas au droit des individus au respect de leur vie privée et familiale une atteinte disproportionnée aux buts de protection de la sécurité publique en vue desquels a été pris le décret ».

841. Le Conseil d'État a également usé de son contrôle de proportionnalité dans le cadre d'une décision portant sur un le fichier dénommé TES[2456]. Le décret du 28 octobre 2016[2457] autorisant sa création avait fait l'objet d'un recours pour excès de pouvoir contestant la légalité du fichier dans un arrêt du 18 octobre 2018[2458]. Le juge administratif a estimé que « l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités »[2459]. Selon lui, « la collecte des images numérisées du visage et des empreintes digitales des titulaires de passeports ou de cartes nationales d'identité […] et la centralisation de leur traitement informatisé […] sont en adéquation avec les finalités légitimes […] de protection de

---

[2454] Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°113 du 16 mai 2007 [en ligne] et Décret n° 2008-631 du 27 juin 2008 portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978, *JORF* n°0152 du 1 juillet 2008 [en ligne].

[2455] Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux.

[2456] Titres électroniques sécurisés : ce fichier permet l'identification des personnes à partir de données biométriques (reconnaissance faciale et empreintes digitales).

[2457] Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, *JORF* n°0254 du 30 octobre 2016 [en ligne].

[2458] CE, 10ème - 9ème ch. réunies, 18 octobre 2018, n° 404996, *Fichier TES* [en ligne].

[2459] *Idem*, § 11.

l'ordre public »[2460]. Dès lors, il a validé la légalité du fichier.

842. Enfin, dans le cadre de sa décision du 22 décembre 2020 portant sur la surveillance des manifestations par les forces de l'ordre au moyen de drones aériens à l'automne 2020[2461], le Conseil d'État, saisi d'un recours en référé-liberté, laisse transparaitre un contrôle de proportionnalité restreint au seul critère de nécessité. En l'espèce, l'association requérante, *La Quadrature du Net*, considérait que la décision de la préfecture de police de Paris avait été prise alors « qu'aucune des finalités poursuivies par le dispositif ne requière la possibilité de capter des images par drones » et que dès lors « le traitement de données personnelles [est] disproportionné »[2462]. Elle contestait ainsi la nécessité de la mesure mise en œuvre et le caractère disproportionné du traitement de DACP. De fait, le principe de proportionnalité transparaît dans les dispositions des textes européens et nationaux relatifs à la protection des DACP au travers du principe de minimisation qui exige que les données soient collectées de manière « non excessive »[2463]. Le Conseil d'État a convenu que les conditions de nécessité de la mise en œuvre de ces dispositifs n'étaient pas remplies considérant le nombre de personnes concernées par cette surveillance et les atteintes engendrées sur leur liberté de manifestation[2464]. Dès lors, il a admis que le principe de proportionnalité n'avait pas été respecté, estimant que « le ministre n'apporte pas d'élément de nature à établir que l'objectif de garantie de la sécurité publique lors de rassemblements de personnes sur la voie publique ne pourrait être atteint pleinement, dans les circonstances actuelles, en l'absence de recours à des drones »[2465].

843. Au sein des juridictions ordinaires, le juge administratif fait figure de pionnier en matière de recours au principe de proportionnalité, même sans le nommer expressément. Si le juge judiciaire a tardé à mettre en œuvre un contrôle de proportionnalité celui-ci l'a désormais ancré dans sa jurisprudence. Au pénal, la chambre criminelle de la Cour de cassation a déjà intégré ce principe pour contrôler les mesures de police judiciaire.

[2460] *Idem*, § 17.

[2461] CE, 10ème - 9ème ch. réunies, 22 décembre 2020, n°446155, *op. cit.*

[2462] TA Paris, ord., 4 novembre 2020, n° 2017540/3/5, *op. cit.*

[2463] DPJ, art. 4, §1, c) et LIL, art. 4 §3 et 87, al. 2.

[2464] CE, 10ème - 9ème chambres réunies, 22 décembre 2020, n°446155, *op. cit.*, cons. 11.

[2465] *Ibid*.

B. Le principe de proportionnalité dans la jurisprudence du juge judiciaire

844. Le contrôle de proportionnalité s'est progressivement généralisé au sein de la jurisprudence judiciaire, d'abord dans le domaine pénal puis dans d'autres domaines[2466]. Aujourd'hui, le principe de proportionnalité est fréquemment appliqué par la Cour de cassation dès qu'une mesure permet de restreindre l'exercice d'un droit ou d'une liberté[2467]. Elle l'applique notamment dans le domaine civil en matière de droit à la preuve qu'elle fonde sur l'article 6 § 1 de la Conv.EDH lorsqu'il se confronte au droit au respect de la vie privée[2468]. Afin d'assurer un juste équilibre entre les deux droits, le juge judiciaire a eu recours au principe de proportionnalité en énonçant que « le droit à la preuve ne peut justifier la production d'éléments portant atteinte à la vie privée qu'à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi »[2469].

845. La Cour de cassation a fréquemment eu recours au principe de proportionnalité en droit pénal[2470]. La généralisation de ce principe au sein de la jurisprudence de la chambre criminelle s'explique notamment au travers de l'article préliminaire du CPP[2471] disposant que « les mesures de contraintes dont la personne suspectée ou poursuivie peut faire l'objet […] doivent être strictement limitées aux nécessités de la procédure [et] proportionnées à la gravité de l'infraction reprochée »[2472]. Elle a notamment eu l'opportunité d'assurer un contrôle de proportionnalité d'actes de police dans différentes affaires. À titre d'exemple, dans un arrêt du 15 novembre 2016, la chambre criminelle a analysé le caractère proportionné d'une mesure d'extradition[2473]. De même,

---

2466 BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 231. Voir aussi : VIGNEAU (V.), « Libres propos d'un juge sur le contrôle de proportionnalité », *Recueil Dalloz*, 2017, p. 123.

2467 DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 169.

2468 *Idem*, p. 335.

2469 C. cass., 1ère ch. civ., 25 février 2016, n° 15-12.403 [en ligne].

2470 BOUCHET (M.), « L'utilisation du contrôle de proportionnalité par la Cour de cassation en droit pénal de fond », *RSC* n° 3, 10 novembre 2017, p. 495.

2471 VERGÈS (É.), *Procédure pénale*, *op. cit.*, p. 63.

2472 CPP, art. préliminaire, III.

2473 C. cass., ch. crim., 15 novembre 2016, n° 16-85.335 [en ligne] : En l'espèce, la Cour de cassation avait estimé que la mesure d'extradition était disproportionnée au regard du droit à la vie privée et familiale de la personne mise en cause.

dans un arrêt du 11 janvier 2017, elle a vérifié que le mandat d'arrêt n'était pas disproportionné au regard des droits et libertés de la personne mise en cause[2474].

846. Dans un arrêt du 11 décembre 2018[2475], la Cour de cassation a effectué un contrôle de proportionnalité pour déterminer si la mesure de surveillance au moyen d'une caméra filmant une portion de la voie publique était nécessaire au regard de l'atteinte qu'elle portait au droit à la vie privée sur le fondement de l'article 8 de la Conv.EDH. Les premiers juges ont admis qu'un dispositif de captation d'images prises sur la voie publique était susceptible de constituer une ingérence dans le droit à la vie privée « dès lors qu'il donne lieu à un enregistrement et permet de retracer les déplacements d'une personne déterminée »[2476]. Cependant, ils ont estimé que « l'ingérence dans la vie privée des requérants […] était nécessaire pour identifier les auteurs des importations de produits stupéfiants et localiser le lieu de stockage de la drogue [et] que cette mesure était également proportionnée à la gravité et à l'importance des infractions objets de l'enquête »[2477]. La Cour de cassation a confirmé la décision de la Cour d'appel concernant le caractère proportionné du recours à ce dispositif.

847. Le principe de proportionnalité, au travers du critère de nécessité, s'est également imposé s'agissant du recours à des drones aériens par la police judiciaire dans le cadre d'une enquête portant sur un trafic de stupéfiants dans un arrêt de la Cour de cassation du 15 novembre 2022[2478] qui statuait pour la première fois sur ce sujet[2479]. En l'espèce, le mis en cause avait avancé le moyen selon lequel « il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée qu'autant que celle-ci est prévue par la loi et nécessaire »[2480]. À l'appui, il avait estimé que l'absence de démonstration de la nécessité de recourir à un dispositif mobile de captation d'images plutôt qu'à un dispositif moins intrusif au regard des circonstances rendait la

---

2474 C. cass., ch. crim., 11 janvier 2017, n° 16-80.619 [en ligne] : La Cour de cassation avait considéré que la décision contestée était invalide dans la mesure où la Cour d'appel n'avait pas « appréci[é] le caractère nécessaire et proportionné du recours à cette mesure de contrainte en fonction des circonstances de l'espèce ».

2475 C. cass., ch. crim., 11 décembre 2018, n° 18-82.365, *op. cit.*

2476 *Ibid*.

2477 *Ibid*.

2478 C. cass., 15 novembre 2022, n° 22-80.097, *op. cit.*

2479 PIGNATEL (L.), « Pas de nullité de principe des opérations de captation d'images réalisés par drone », *Dalloz act.* n° 29, 29 novembre 2022. Voir aussi: COLLET (P.), « Le recours aux drones validé pour la criminalité organisée ! », *JCP G* n° 1, 9 janvier 2023, act. 18.

2480 C. cass., 15 novembre 2022, n° 22-80.097, *op. cit.*, § 5.

mesure employée disproportionnée. Le juge judiciaire examinant les critères de nécessité et de proportionnalité de la mesure a rappelé que la collecte de données par un tel dispositif est constitutive d'une ingérence dans le droit à la vie et que toute mesure de police judiciaire doit être justifiée par une base légale ainsi que la poursuite d'un but légitime[2481]. En l'espèce, il a estimé que dans la mesure où « le magistrat a rappelé comment le trafic a été mis en évidence et pourquoi les lieux désignés ont été ciblés par les enquêteurs »[2482] et que « le juge d'instruction, relevant que la configuration de ces mêmes lieux rendait toute surveillance difficile, a exposé les motifs pour lesquels ces investigations sont indispensables à la manifestation de la vérité »[2483] le recours à ce dispositif par la police judiciaire était proportionné. Cependant, il convient de garder à l'esprit que cette solution portait sur une mesure en matière de criminalité organisée et qu'elle poursuivait un but légitime d'enquête[2484].

848. Bien au-delà de l'application qu'en fait le juge judiciaire, le contrôle de proportionnalité se trouve au cœur de la jurisprudence du Conseil constitutionnel, largement inspirée par celle de la cour constitutionnelle fédérale allemande puis par celle des juges européens[2485].

C. Le recours au contrôle de proportionnalité par le juge constitutionnel

849. L'émergence du principe de proportionnalité dans la jurisprudence constitutionnelle - En dépit de l'absence de mention explicite du principe de proportionnalité dans le texte de la Constitution de 1958[2486], le Conseil constitutionnel exerce depuis longtemps un contrôle de proportionnalité des dispositions qui sont soumises à son examen. Dès ses premières

---

[2481] *Idem*, § 7.

[2482] *Idem*, § 18.

[2483] *Idem*, § 19.

[2484] PIGNATEL (L.), « Pas de nullité de principe des opérations de captation d'images réalisés par drone », *op. cit.*

[2485] FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, *op. cit.*, p. 858 ; ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 365 ; GOSEL-LE BIHAN (V.), « Le contrôle de proportionnalité au Conseil constitutionnel », *AJDA* n° 14, 19 avril 2021, p. 786.

[2486] Voir en ce sens les analyses du bloc de constitutionnalité effectuées par le professeur Xavier Philippe (PHILIPPE (X.), *Le contrôle de proportionnalité dans les jurisprudences constitutionnelle et administrative*, *op. cit.*, pp. 124 et suiv.) et par Marc-Antoine Granger dans leur thèse respective concernant la recherche du principe de proportionnalité (GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, pp. 292-295). Les auteurs avaient identifié la présence implicite du principe de proportionnalité au travers de l'exigence de nécessité régulièrement mentionnée dans les textes constitutionnels. À ce titre, le professeur Xavier Philippe était parvenu à la conclusion que les notions de nécessité et de proportionnalité étaient étroitement liées et pouvaient même se substituer (pp. 88-91).

décisions, le juge constitutionnel a mis en œuvre ce contrôle portant sur la conciliation entre deux normes constitutionnelles[2487]. Ainsi, dans sa décision du 25 juillet 1979[2488], le Conseil constitutionnel a énoncé que le droit de grève, reconnu par le Préambule de la Constitution du 27 octobre 1946[2489], a des limites et qu' « il appartient au législateur […] de le concilier avec le principe de la continuité du service public »[2490]. Pour la première fois, le juge constitutionnel a exercé son contrôle de proportionnalité en s'assurant que le législateur avait respecté son devoir d'opérer une conciliation « équilibrée » entre deux normes de valeur constitutionnelle. En matière de contentieux de la police, le Conseil constitutionnel, dans sa décision du 25 janvier 1985[2491], a formulé pour la première fois l'exigence de conciliation du législateur entre deux principes ou deux dispositions de valeur constitutionnelle pour exprimer son contrôle de proportionnalité[2492]. Par la suite, ce contrôle de proportionnalité reposant sur l'exigence de conciliation du législateur entre les droits et libertés constitutionnellement garantis, d'une part, et les objectifs de sauvegarde de l'ordre public et de la recherche des auteurs d'infractions, d'autre part, est devenu une constante dans la jurisprudence du Conseil constitutionnel[2493] (v. **n° 854 et suiv.**).

850. Le principe de proportionnalité fut expressément mentionné pour la première fois[2494] par le juge constitutionnel dans une décision du 28 juillet 1989 énonçant qu'il « implique qu'en tout état de cause, le montant global des sanctions éventuellement prononcées ne dépasse pas le montant le plus élevé de l'une des sanctions encourues »[2495]. Il s'est progressivement concrétisé lorsque le juge a eu à contrôler des limitations portées à des droits ou libertés pour déterminer si elles étaient justifiées. Le contrôle de proportionnalité exercé par le juge constitutionnel s'est banalisé mais ce

---

[2487] GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, p. 180.

[2488] C. const., Décision n° 79-105 DC, 25 juillet 1979, *Loi modifiant les dispositions de la loi n° 74-696 du 7 août 1974 relatives à la continuité du service public de la radio et de la télévision en cas de cessation concertée du travail*, Rec. p. 33 [en ligne].

[2489] *Idem*, cons. 1.

[2490] *Idem*, cons. 3.

[2491] C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.*, cons. 3 et 4 : « En vertu de l'article 34 de la Constitution la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Dans ce cadre, il appartient au législateur d'opérer la conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public sans lequel l'exercice des libertés ne saurait être assuré ».

[2492] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 306.

[2493] *Ibid*. À titre d'exemple : C. const., Décision n° 2005-532 DC, 19 janvier 2006, *op. cit.*, cons. 21 ; C. const., Décision n° 2015-713 DC, 23 juillet 2015, *op. cit.*, spéc. cons. 56 et 67 ; C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.*, cons. 88, 96, 101, 114, 141, 148 et 183.

[2494] ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 364.

[2495] C. const., Décision n° 89-60 DC, 28 juillet 1989, *op. cit.*, cons. 22.

dernier en fait toutefois varier l'intensité selon le domaine concerné, les types de droits et libertés impliqués, ou encore les garanties prévues[2496]. En ce sens, la jurisprudence du Conseil constitutionnel est rigoureuse en matière de protection des DACP, considérant de manière constante que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif »[2497].

851. Le renforcement du contrôle de proportionnalité du juge constitutionnel - Dans le cadre de sa décision du 21 février 2008[2498] portant sur la rétention de sûreté, le juge constitutionnel a consacré le principe de proportionnalité en venant préciser les critères de son contrôle. À cette occasion, il avait jugé du caractère potentiellement attentatoire de ces mesures à la liberté individuelle. Aujourd'hui, cette liberté a été classée dans la catégorie des droits jugés essentiels faisant l'objet d'un contrôle strict par le Conseil constitutionnel[2499]. Depuis lors, le juge constitutionnel assure le respect du principe de proportionnalité des lois restrictives des libertés[2500] qui lui sont soumises en les soumettant à un contrôle en vue de déterminer si les mesures qu'elles mettent en œuvre sont « adaptées, nécessaires et proportionnées »[2501]. Ce triple test de proportionnalité démontre l'intensité du contrôle exercé par le Conseil constitutionnel pour garantir les droits et libertés en cause[2502]. Celui-ci peut aussi s'accompagner de réserves d'interprétation destinées à orienter les autorités publiques qui mettent en œuvre la loi[2503].

2496 Voir notamment : ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 365 ; BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, *op. cit.*, p. 302.

2497 À titre d'exemple : C. const., Décision n° 2012-652 DC, 22 mars 2012, *op. cit.*, cons. 8 ; C. const., Décision n° 2021-819 DC, 31 mai 2021, *Loi relative à la gestion de la sortie de crise sanitaire*, *JORF* n°0125 du 1 juin 2021, texte n° 2, cons. 24 [en ligne].

2498 C. const., Décision n°2008-562 DC, 21 février 2008, *op. cit.*, cons. 13 à 23.

2499 GOSEL-LE BIHAN (V.), « Le contrôle de proportionnalité au Conseil constitutionnel », *op. cit.*

2500 SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

2501 STIRN (B.), « Ordre public et libertés publiques », p. 11 *in* SÈVE (R.), *L'ordre public*, *op. cit.* Le Conseil constitutionnel a confirmé le recours à ce triple test de proportionnalité dans ses décisions de contrôle *a priori* (C. const., Décision n° 2011-631 DC, 9 juin 2011, *Loi relative à l'immigration, à l'intégration et à la nationalité*, Rec. p. 252, cons. 66 [en ligne]) et de contentieux relatif aux questions préjudicielles de constitutionnalité (ex. C. const., Décision n° 2012-253 QPC, 8 juin 2012, *M. Mickaël D*, Rec. p. 289 [en ligne]).

2502 GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, *op. cit.*, p. 179 et suiv.

2503 BIOY (X.), *Droits fondamentaux et libertés publiques*, *op. cit.*, p. 230.

852. Le Conseil constitutionnel n'applique pas le triple test de proportionnalité de manière identique d'une décision à l'autre[2504], son contrôle variant notamment en fonction du type de droits ou libertés en cause. À l'origine, le triple test avait été réservé à deux libertés : la liberté individuelle et la liberté de communication[2505]. Par la suite, ce contrôle s'est étendu à la liberté de manifestation[2506] puis à celle de réunion[2507]. Aujourd'hui, ce contrôle approfondi de proportionnalité est appliqué à d'autres libertés individuelles.

853. Autrefois réservé aux seules privations de libertés, le juge constitutionnel a aussi eu recours au triple test de proportionnalité pour examiner des mesures de police judiciaire restrictives de la liberté personnelle dans sa décision du 7 août 2020[2508], élargissant ainsi son contrôle approfondi de proportionnalité à la liberté d'aller et venir, au droit au respect de la vie privée et au droit au respect de la vie familiale. Néanmoins, le juge constitutionnel réserve ce contrôle aux seules mesures de police judiciaire, excluant par conséquent les mesures de police administrative, alors que son contrôle était déjà restreint en la matière[2509]. Pourtant les mesures de police administrative mériteraient également de faire l'objet d'un contrôle approfondi de proportionnalité tant leur champ d'action s'est étendu notamment s'agissant des mesures en matière de lutte contre les menaces terroristes[2510]. En ce sens, le phénomène de « judiciarisation » de la police administrative[2511], décrit par Marc-Antoine Granger, démontre l'amplification des prérogatives accordées aux forces de police administratives sans qu'un contrôle préalable du juge ne soit nécessaire (à l'inverse de la police judiciaire). Dès lors, la souplesse du contrôle de proportionnalité du Conseil constitutionnel à l'égard des mesures de police administratives ne permet pas de

---

2504 DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, *op. cit.*, p. 168 ; ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 366.

2505 GOSEL-LE BIHAN (V.), « Le contrôle de proportionnalité au Conseil constitutionnel », *op. cit.*

2506 C. const., Décision n° 2019-780 DC, 4 avril 2019, *Loi visant à renforcer et garantir le maintien de l'ordre public lors des manifestations*, *JORF* n°0086 du 11 avril 2019 , texte n° 2, cons. 13 à 16 [en ligne].

2507 C. const., Décision n° 2020-803 DC, 9 juillet 2020, *Loi organisant la sortie de l'état d'urgence sanitaire*, *JORF* n°0169 du 10 juillet 2020, texte n° 2, cons. 20 à 26 [en ligne].

2508 C. const., Décision n° 2020-805 DC, 7 août 2020, *Loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine*, *JORF* n°0196 du 11 août 2020, texte n° 4, cons. 10 [en ligne]

2509 GOSEL-LE BIHAN (V.), « Le contrôle de proportionnalité au Conseil constitutionnel », *op. cit.*

2510 Voir notamment : Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, *op. cit.* ; Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, *op. cit.*

2511 GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, pp. 191-222.

renforcer avec certitude les garanties que cette technique peut conférer aux droits et libertés. Quelques exemples permettent d'illustrer le propos.

854. L'application du contrôle de proportionnalité aux mesures de police - Dans sa décision du 18 janvier 1995[2512], le juge constitutionnel a examiné la nécessité et la proportionnalité, notamment du recours à des caméras filmant la voie publique. Les requérants ont fait valoir que compte tenu des restrictions que portaient ces dispositifs à la liberté d'aller et venir et au droit à la vie privée, les dispositions contestées n'apportaient pas de garanties suffisantes[2513]. Le juge constitutionnel a rappelé « qu'il appartient au législateur d'assurer la conciliation entre ces objectifs de valeur constitutionnelle et l'exercice des libertés publiques constitutionnellement garanties au nombre desquelles figurent la liberté individuelle et la liberté d'aller et venir ainsi que l'inviolabilité du domicile »[2514]. Lors de son contrôle, il a simplement exigé que « la mise en œuvre de systèmes de vidéosurveillance [soit] assortie de garanties de nature à sauvegarder l'exercice de ces libertés individuelles »[2515].

855. Lors de leur décision du 2 mars 2004[2516] concernant la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité[2517], les Sages ont examiné la constitutionnalité des dispositions procédurales dérogatoires applicables à la criminalité organisée. À cette occasion, le juge constitutionnel a rappelé que le législateur était tenu « d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions […] et, d'autre part, l'exercice des libertés constitutionnellement garanties »[2518]. Il a considéré que la mise en œuvre de mesures d'investigations spéciales pouvait être autorisée par le législateur sous réserve que les restrictions portées aux libertés constitutionnellement garanties

---

[2512] C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.*

[2513] *Idem*, cons. 2.

[2514] *Idem*, cons. 3.

[2515] *Idem*, cons. 3 et 4.

[2516] C. const., Décision n° 2004-492 DC, 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité, op. cit.*

[2517] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, *op. cit.*

[2518] C. const., Décision n° 2004-492 DC, *op. cit*., cons. 4 et 76.

respectent les principes de nécessité et de proportionnalité[2519]. Le Conseil constitutionnel exerce ainsi un contrôle restreint de ces mesures, tenant compte du fait qu'elles portent sur des infractions graves pour l'ordre public[2520].

856. Dans le cadre d'une question prioritaire de constitutionnalité du 24 juillet 2015, le juge constitutionnel a examiné la réquisition généralisée de données de connexion par les forces de l'ordre[2521]. Les requérants contestaient la validité des dispositions du CSI estimant que le législateur n'avait pas prévu de garanties adaptées et que par conséquent ces mesures constituaient une atteinte au droit à la vie privée et au droit au secret des correspondances[2522]. Le Conseil constitutionnel a reconnu l'ingérence dans le droit à la vie privée mais a rejeté la reconnaissance constitutionnelle d'un droit au secret et des correspondances[2523]. Il a considéré après un examen des conditions de mise en œuvre de ces mesures qu'en raison de leurs finalités de sécurité nationale et dans la mesure où les données de connexion réquisitionnées ne permettaient pas d'accéder au contenu des correspondances, celles-ci ne portaient pas une atteinte disproportionnée aux différents droits mentionnés[2524].

857. Le contrôle de proportionnalité est donc solidement ancré dans la jurisprudence nationale et européenne et permet notamment de limiter les restrictions portées aux droits et libertés par les mesures de police. Toutefois, face à l'insuffisance de motivation des décisions du Conseil constitutionnel, certains auteurs appellent « un effort de pédagogie et de précision de la motivation […] d'autant plus qu'un contrôle effectué de manière précise est généralement synonyme d'une garantie davantage effective des droits et libertés »[2525].

[2519] *Idem*, cons. 6 : « le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs, […] sous réserve que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire, gardienne de la liberté individuelle, et que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient nécessaires à la manifestation de la vérité, proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées ».

[2520] *Idem*, cons. 47.

[2521] C. const., Décision n° 2015-478 QPC, 24 juillet 2015, *Association French Data Network et autres*, *op. cit.*

[2522] *Idem*, cons. 14.

[2523] *Idem*, cons. 16.

[2524] *Idem*, cons. 17, 18 et 19.

[2525] ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, *op. cit.*, p. 367.

Section 2 Un nécessaire renforcement du contrôle de la proportionnalité du recours aux technologies de surveillance « augmentées » de sécurité publique

858. Le recours au contrôle de proportionnalité au sein de la jurisprudence européenne et nationale contribue indéniablement au renforcement des garanties des droits et libertés. Pour autant, si sa présence s'est globalement généralisée, il apparait que les juges, tant européens que nationaux, laissent encore une large marge d'appréciation aux autorités publiques[2526]. Dès lors, le constat est fait d'une relativité du contrôle de proportionnalité des mesures prises en matière de sécurité, publique comme nationale, notamment s'agissant du recours à des caméras de vidéoprotection (§1). L'arrivée des technologies de surveillance « augmentées » à l'usage des forces de l'ordre appelle donc l'application d'un contrôle strict et approfondi de proportionnalité de la part des juges nationaux mais aussi européens. Toutefois, si le principe de proportionnalité a sa place dans la jurisprudence, il doit s'exprimer de manière additionnelle dans les dispositions législatives et les mesures de police et pourrait notamment bénéficier d'une implication préalable étendue des citoyens dans le processus de choix des technologies et de leurs usages par les forces de l'ordre (§2).

§1. La relativité des contraintes du contrôle de proportionnalité sur les technologies de sécurité publique

859. La pratique du contrôle de proportionnalité au sein de la jurisprudence nationale laisse apparaitre une certaine nuance tant dans son intensité que dans sa précision (A). Plus spécifiquement, dans le cadre des décisions portant sur les caméras de vidéoprotection, le contrôle de proportionnalité peine à convaincre de son efficacité à garantir de manière effective l'exercice des droits et libertés (B).

[2526] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.* ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 150.

A. Le caractère fluctuant du contrôle de proportionnalité

860. Le vice-président du Conseil d'État, Jean-Marc Sauvé, déclarait que le principe de proportionnalité était « indispensable à la garantie de l'État de droit »[2527]. Néanmoins, les études portant sur le contrôle de proportionnalité font régulièrement état de sa souplesse et de sa variabilité[2528]. En ce sens, la doctrine est relativement unanime pour affirmer que le contrôle de proportionnalité exercé par les juridictions nationales n'est « jamais complètement restreint, jamais complètement entier »[2529] et qu'il se mesure selon les circonstances de l'espèce.

861. En matière de contrôle de proportionnalité des technologies de sécurité publique, il n'est pas toujours possible d'identifier ce que Marc-Antoine Granger qualifiait dans sa thèse de « balises » d'identification de la variabilité de l'intensité du contrôle de proportionnalité effectué par le Conseil constitutionnel[2530]. L'exercice du contrôle de proportionnalité, s'il est essentiel à la garantie des droits et libertés, nécessite, de fait, de prendre quelques précautions que Jean-Marc Sauvé a détaillé lors de son discours à la conférence du 17 mars 2017. Il énonçait que ce contrôle devait « être stable et cohérent pour être prévisible », reposer « sur une motivation explicite et rigoureuse » et effectuer une réelle « mise en balance des différents intérêts en présence et non [assurer] la prédominance systématique des droits fondamentaux sur l'intérêt général »[2531].

862. L'affaiblissement du contrôle de proportionnalité exercé par les différentes juridictions, souvent au prétexte de « l'importance vitale » de lutte contre les menaces terroristes, met en lumière le besoin de revoir son mode d'application afin d'assurer une garantie effective des droits et libertés. Ce renforcement s'impose tout particulièrement à l'heure où les technologies de surveillance à des fins de sécurité publique intègrent progressivement des algorithmes d'IA. À cette fin, il apparait que seul un examen par le juge constitutionnel « au cas par cas, liberté par liberté, dispositif policier par

---

[2527] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

[2528] Voir notamment : PHILIPPE (X.), *Le contrôle de proportionnalité dans les jurisprudences constitutionnelle et administrative*, *op. cit.*, p. 492 ; GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *op. cit.*

[2529] FRAISSE (R.), « Le Conseil constitutionnel exerce un contrôle conditionné, diversifié et modulé de la proportionnalité », *LPA* n° 46, 5 mars 2009, p. 74.

[2530] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 320.

[2531] SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *op. cit.*

dispositif policier »[2532] permettrait de garantir un contrôle suffisant des mesures restrictives des droits et libertés. C'est ce que rappelle en substance le rapport du député Jean-Michel Mis s'agissant des principes de proportionnalité et de nécessité qui, « selon la CNIL, imposent des analyses au cas par cas appliquées *in concreto* à des usages bien déterminés »[2533]. Néanmoins, l'étude de la jurisprudence du juge constitutionnel permet de constater que les dispositions relatives aux systèmes de vidéoprotection (fixes et aéroportés) ont systématiquement fait l'objet de son contrôle préalable examinant la proportionnalité des mesures adoptées[2534]. Cependant, si le contrôle de proportionnalité du Conseil constitutionnel s'est effectivement exercé au cas par cas pour chaque dispositif de vidéoprotection, force est de constater qu'il effectue un examen encore limité de la conciliation effectivement opérée par le législateur entre les droits et libertés constitutionnellement garantis, d'une part, et les mesures répondant aux objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, d'autre part.

B. L'insuffisance du contrôle de proportionnalité du recours aux technologies de surveillance de sécurité publique

863. Le Conseil constitutionnel exerce un contrôle de proportionnalité, presque systématique, des dispositions relatives à la sécurité publique ou intérieure[2535]. Cette technique essentielle en vue de garantir de manière effective l'exercice des droits et libertés peut néanmoins se révéler insuffisante suivant l'intensité du contrôle exercé. En dépit des réserves d'interprétation du juge constitutionnel, l'intensité de ce contrôle ne donne pas entière satisfaction en matière de dispositifs policiers de traitement des DACP dans la mesure où il se montre tantôt plus exigeant tantôt plus permissif. D'une part, le Conseil constitutionnel exerce un contrôle strict à l'égard des dispositions autorisant le recours à des dispositifs policiers de traitement de DACP[2536] (v. **n° 850**). D'autre part, il est contraint par son principe affirmant qu'il « ne dispose pas d'un pouvoir général d'appréciation

---

[2532] GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, *op. cit.*, p. 325.

[2533] Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 45.

[2534] C. const., Décision n° 94-352 DC, 18 janvier 1995, *op. cit.* (LOPS) ; C. const., Décision n° 2011-625 DC, 10 mars 2011, *op. cit.* (LOPPSI) ; C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.* ; C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.* (RPSI) ; C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.* (JOP2024).

[2535] À titre d'exemple : C. const., Décision n° 85-187 DC, 25 janvier 1985, *op. cit.* (état d'urgence) ; C. const., Décision n° 2003-467 DC, 13 mars 2003, *op. cit.* ; C. const., Décision n° 2005-532 DC, 19 janvier 2006, *op. cit.* ; C. const., Décision n° 2015-713 DC, 23 juillet 2015, *op. cit.*

[2536] Voir notamment : C. const., Décision n° 2018-765 DC, 12 juin 2018, *op. cit.*

et de décision de même nature que celui du Parlement. Il ne lui appartient donc pas de rechercher si l'objectif que s'est assigné le législateur n'aurait pas pu être atteint par d'autres voies, dès lors que les modalités retenues par la loi ne sont pas manifestement inappropriées à l'objectif »[2537]. Ces variations d'intensité du contrôle de proportionnalité exercé par le Conseil constitutionnel se retrouvent aussi dans ses dernières décisions portant sur des dispositifs de vidéoprotection.

864. Dans sa décision du 20 mai 2021, le juge constitutionnel a effectué le contrôle de constitutionnalité de plusieurs dispositions de la loi dite « Sécurité globale », dont certaines portaient sur le recours à des dispositifs de captation d'images à des fins de sécurité publique[2538]. D'une manière générale, le contrôle de proportionnalité opéré sur ces dispositifs par les Sages se révèle satisfaisant. En ce sens, il a reconnu que le législateur avait opéré une conciliation équilibrée s'agissant des dispositions autorisant le recours par les agents des forces de l'ordre à des caméras individuelles[2539]. À cette fin, il s'est assuré que la captation des images était limitée dans le temps à l'intervention en cours, que l'information délivrée aux personnes concernées était proportionnée aux circonstances de leur utilisation par une formulation verbale ainsi qu'un signal visuel et que leur transmission en temps réel était limitée aux cas où l'intégrité physique des personnes était menacée[2540].

865. Dans cette même décision, il a frappé d'inconstitutionnalité les dispositions relatives à l'usage de caméras embarquées dans des véhicules, aéronefs, ou autres moyens de transport des forces de l'ordre estimant qu'elles méconnaissaient le droit au respect de la vie privée[2541]. Il a ainsi considéré qu'elles permettaient, au besoin, la captation d'images de l'intérieur d'un bâtiment ou de son entrée, que l'obligation d'information était insuffisante, que la durée et l'étendue maximales de la surveillance n'avaient pas été fixées, et que leur emploi n'était soumis à aucune autorisation d'une quelconque autorité[2542]. Aussi, s'agissant des dispositions portant sur la captation d'images au moyen d'aéronefs circulant sans personne à bord, le juge constitutionnel les a reconnues comme

---

[2537] La formulation de ce principe est apparue pour la première fois dans la décision IVG du 15 janvier 1975 (C. const., Décision n° 74-54 DC du 15 janvier 1975, *Loi relative à l'interruption volontaire de la grossesse*, Rec. p. 19, cons. 1 [en ligne].

[2538] C. const., Décision n° 2021-817 DC, 20 mai 2021, *op. cit.*

[2539] *Idem*, cons. 114.

[2540] *Idem*, cons. 110 à 113.

[2541] *Idem*, cons. 148.

[2542] *Idem*, cons. 147 et 145.

étant disproportionnées au regard de l'atteinte qu'elles portaient au droit au respect de la vie privée[2543]. Il a tout d'abord reconnu qu' « eu égard à leur mobilité et à la hauteur à laquelle ils peuvent évoluer, ces appareils sont susceptibles de capter […] des images d'un nombre très important de personnes et de suivre leurs déplacements dans un vaste périmètre »[2544]. Il a donc effectué son contrôle de proportionnalité en procédant à une analyse des garanties mises en œuvre par le législateur. Après avoir constaté la légitimité du recours à cette technologie par les forces de l'ordre[2545], il a reconnu le caractère disproportionné de leur emploi à des fins de surveillance des manifestations au sein de l'espace public[2546] sans pour autant examiner plus avant les différentes finalités prévues par le législateur. Le Conseil constitutionnel s'est ensuite limité à soulever l'absence de mention par le législateur de la durée et du périmètre maximales de la surveillance ainsi que du nombre de drones aériens pouvant être déployés simultanément[2547].

866. En revanche, dans sa décision du 20 janvier 2022 portant sur la loi RPSI[2548], le Conseil constitutionnel, exerçant un contrôle des dispositions relatives au recours à la captation d'images au moyen d'aéronefs circulant sans personne à bord par les forces de l'ordre, a fait preuve de moins d'exigence quant au devoir de conciliation du législateur et ce à plusieurs égards. En premier lieu, il n'a envisagé que l'interdiction de la collecte et du traitement des données permettant d'effectuer une reconnaissance faciale par les drones aériens à l'usage des forces de l'ordre[2549], excluant ainsi d'autres types de données à caractère biométriques, tels la démarche. En deuxième lieu, il n'a pas jugé utile d'effectuer un contrôle de proportionnalité des finalités de leur recours et de leur caractère parfois inadapté à ce dispositif de surveillance[2550], notamment au regard de leur caractère particulièrement intrusif pour la vie privée. De fait, certaines finalités, plus spécifiquement celles visant à prévenir les actes de terrorisme, auraient mérité de faire l'objet d'un contrôle de proportionnalité approfondi. De fait, en raison du caractère illimité dans le temps et dans l'espace de ces menaces sur l'ordre public, cette finalité ne permet pas de manière concrète d'envisager un usage

---

[2543] *Idem*, cons. 141.

[2544] *Idem*, cons. 135.

[2545] *Idem*, cons. 137.

[2546] *Idem*, cons. 139.

[2547] *Idem*, cons. 138 et 140.

[2548] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*

[2549] *Idem*, cons. 30.

[2550] Voir en ce sens : CSI, art. L. 242-5 (drones aériens) et art. L. 251-2 (caméras fixes).

des drones aériens conciliant les objectifs de sauvegarde de l'ordre public et de la recherche des auteurs d'infractions, d'une part, et la protection des droits et libertés, d'autre part. Néanmoins, il convient de saluer la clairvoyance du juge constitutionnel qui a reconnu que l'usage de ces dispositifs en cas d'urgence sans autorisation préalable du préfet ne permettait pas d'assurer une conciliation équilibrée[2551].

867. Dans sa décision du 17 mai 2023, le Conseil constitutionnel a effectué un contrôle de constitutionnalité de la loi JOP2024 introduisant notamment des dispositions provisoires permettant l'expérimentation de caméras « augmentées » fixes et mobiles filmant la voie publique[2552]. Cette décision se distingue des précédentes s'agissant du recours à des drones aériens dans la mesure où plusieurs droits constitutionnellement garantis ont été invoqués pour contester les dispositions de ce texte[2553]. Cependant, le juge constitutionnel n'a pas saisi l'opportunité d'effectuer son contrôle de proportionnalité au regard de chaque droit invoqué se contentant simplement de mentionner le droit à la vie privée[2554]. Il est regrettable que le Conseil constitutionnel n'ait pas reconnu la durée de l'expérimentation comme étant disproportionnée, se satisfaisant de la mention par le législateur de la durée maximale de l'expérimentation[2555]. Aussi, il faut espérer que l'exclusion expresse de tout traitement de données à caractère biométrique du texte de loi[2556] incite le juge constitutionnel à la vigilance dans l'éventualité où d'autres technologies de surveillance élargiraient leur traitement à ce type. Enfin, si le Conseil constitutionnel a validé la constitutionnalité du texte, il a toutefois précisé que dans le cas où ces technologies viendraient à être pérennisées celui-ci assurerait un contrôle des dispositions autorisant leur mise en œuvre à l'appui des conclusions du rapport établi à la fin de la période d'expérimentation[2557].

868. Au vu de ce qui précède, il est possible de conclure au caractère particulièrement incertain du contrôle de proportionnalité des décisions du Conseil constitutionnel en matière de

---

[2551] C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 31.

[2552] C. const., Décision n° 2023-850 DC, 17 mai 2023, *op. cit.*

[2553] *Idem*, cons. 29.

[2554] *Idem*, cons. 46.

[2555] *Idem*, cons. 47.

[2556] *Idem*, cons. 42.

[2557] *Idem*, cons. 48.

dispositifs de surveillance de la voie publique.

§2. Les recommandations pour repenser la proportionnalité du recours aux technologies de surveillance « augmentées » de sécurité publique respectueux des droits et libertés

869. Déjà en 1994, la CNIL avait rappelé avec fermeté que « toute mise en œuvre d'un dispositif de vidéosurveillance des voies publiques, des lieux publics et des lieux recevant du public [doit] respecte[r] le principe de proportionnalité, [celui-ci étant apprécié] au regard de la finalité du système »[2558]. Aussi, la règlementation en matière de protection des DACP mentionne de manière explicite le principe de proportionnalité[2559], notamment au travers de l'article 4 de la DPJ[2560] et de l'article 87 de la LIL[2561]. En outre, elle caractérise son importance au travers d'autres principes exigeant des finalités légitimes[2562] ainsi qu'un traitement « non excessif »[2563] des données en matière de police. Dès lors, le principe de proportionnalité est étroitement lié aux usages de technologies opérant un traitement de DACP. Plusieurs acteurs appellent ainsi à ne pas céder à un recours disproportionné des technologies de surveillance à des fins de sécurité publique (A). Aussi, l'analyse des rapports et études portant sur l'usage de technologies reposant sur de l'IA et, plus spécifiquement, les technologies de surveillance « augmentées » met en lumière l'intérêt d'introduire une participation citoyenne dans le choix de leurs usages (B).

A. L'évidence du principe de proportionnalité en matière de technologies de surveillance de sécurité publique

870. Le caractère proportionnel et nécessaire de l'usage de technologies « augmentées » par les forces de sécurité publique repose, entre autres choses, sur les finalités du traitement des

---

2558 CNIL, Délibération n° 94-056 du 21 juin 1994, *15ème rapport d'activité de la Commission nationale de l'informatique et des libertés pour 1994*, éd. La Documentation française, 1995, p. 378 [en ligne].

2559 RGPD, cons. 4, 19 §2, 50 §2, 73, 129 et 170 ; DPJ, cons. 26, 29, 44, 82 et 93.

2560 DPJ, art. 4, §2 b) : « Le traitement, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 1er, paragraphe 1 [de la DPJ], autre que celles pour lesquelles les données ont été collectées, est autorisé à condition que […] le traitement soit nécessaire et proportionné à cette autre finalité conformément au droit de l'Union ou au droit d'un État membre ».

2561 LIL, art. 87 : Les traitements de DACP effectués dans le cadre des finalités prévues par la DPJ assurent « notamment la proportionnalité de la durée de conservation des données à caractère personnel, compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions concernées ».

2562 DPJ, art. 4, §1 a) et LIL, art. 4, 2).

2563 DPJ, art. 4, §1, c) et LIL, art. 4, 3).

données et notamment sur le type de données collectées. Le traitement de DACP qualifiées de sensibles au sens du RGPD et de la DPJ, telles que les données biométriques, suscite une inquiétude légitime des défenseurs des droits et libertés. Leur traitement par les forces de l'ordre fait par conséquent l'objet d'un encadrement strict qui l'interdit par principe mais qui admet néanmoins des exceptions limitativement énumérées[2564]. Cependant, le recours à des dispositifs biométriques de surveillance de l'espace public viendrait étendre les possibilités d'atteintes aux droits et libertés. Or, à l'exception des dispositifs de reconnaissance faciale, les dispositions relatives à l'usage de drones aériens de sécurité publique n'excluent pas formellement la possibilité d'intégrer un traitement d'autres types de données biométriques[2565]. En outre, s'agissant plus spécifiquement des dispositifs biométriques d'identification en temps réel dans l'espace public, la Défenseure des droits, après avoir rappelé leur caractère très intrusif, considère qu'il est « difficile de concevoir comment l'utilisation de ces systèmes pourrait être considérée comme nécessaire et proportionnée compte tenu des risques de détournement d'usage et de biais qu'ils présentent »[2566]. Pour ces raisons, les institutions européennes ont souhaité exclure les possibilités pour les forces de l'ordre de recourir à la reconnaissance faciale[2567] dans la mesure où de nombreuses associations s'y sont opposées compte tenu de l'ingérence grave qu'elle engendre dans le droit au respect de la vie privée[2568].

871. Ainsi que le rappelle le Conseil d'État dans son étude sur l'IA dans le secteur public, le recours à des technologies « augmentées » requière « une finalité d'intérêt général avérée et que l'ingérence dans les droits et libertés fondamentaux qui [en] résulte [ne soit] pas disproportionnée au regard des bénéfices qui en sont attendus »[2569]. À cette fin, les autorités publiques, sous le contrôle des juges, devront analyser au cas par cas si l'emploi d'une technologie de surveillance « augmentée » de sécurité publique est nécessaire et proportionné au regard des atteintes qu'il peut porter aux droits et libertés[2570]. Dès lors, bien que l'emploi de drones aériens

---

[2564] DPJ, art. 10 et LIL, art. 6.

[2565] Voir en ce sens : CSI, art. L. 242-4, al. 2 ; C. const., Décision n° 2021-834 DC, 20 janvier 2022, *op. cit.*, cons. 30.

[2566] DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », *op. cit.*

[2567] REIA, art. 5.

[2568] Voir notamment : EDRi (European Digital Rights), "Civil society urges European Parliament to protect people's rights in the AI Act", *op. cit.*

[2569] CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, pp. 98-99.

[2570] *Idem*, p. 100 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 150.

« augmentés » de sécurité publique réponde à un objectif d'intérêt général, leur ingérence dans les droits et libertés doit être examiné pour identifier si leur usage est proportionné au regard des objectifs poursuivis. Plusieurs auteurs appellent ainsi de leurs vœux une application du principe de proportionnalité aux systèmes algorithmiques décisionnels ou d'aide à la prise de décision[2571] et plus généralement aux outils de surveillance[2572].

872. Le recours au principe de proportionnalité semble être naturellement lié aux usages technologiques effectuant des traitements de DACP dans la mesure où la règlementation qui les encadre pose indirectement le principe de proportionnalité parmi ses exigences de limitation des données collectées ou encore de limitation de conservation des données[2573]. Il serait approprié de conditionner le recours à des technologies « augmentées » au respect du principe de proportionnalité. En ce sens, l'intégration de ce principe à la règlementation et aux mesures administratives en matière de technologies de surveillance « augmentées » à des fins de sécurité publique permettrait de renforcer la protection des droits et libertés en limitant, voire en prohibant, les usages les plus intrusifs[2574]. De fait, la limitation du pouvoir régalien repose sur le principe de proportionnalité et œuvre ainsi à l'encadrement des usages technologiques en matière de police. Le principe peut toutefois paraître très théorique au point de limiter sa concrétisation en pratique[2575]. Dès lors, certains auteurs ont avancé des outils de mesure de la proportionnalité en vue d'améliorer sa mise en œuvre. Ces outils de mesure reposeraient sur deux critères : l'évaluation de leur efficacité, d'une part, et l'évaluation de leur degré d'intrusion au regard des droits et libertés consacrés par les textes et juridictions nationaux et européens, d'autre part[2576]. Cependant, il convient de relativiser les apports de ce principe compte tenu de la marge d'appréciation étendue laissée aux autorités publiques et du caractère variable du contrôle de proportionnalité exercé par les juges notamment s'agissant des usages des technologies de surveillance à des fins de sécurité publique.

[2571] Voir notamment : MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 387 ; DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, pp. 147-150.

[2572] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 17.

[2573] RGPD, art. 5, c) et e) ; DPJ, art. 4, c) et e) ; LIL, art. 4, 3) et 5).

[2574] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 387

[2575] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, p. 93.

[2576] *Ibid*.

B. L’ouverture du principe de proportionnalité à la participation citoyenne en matière de technologies de surveillance de sécurité publique

873. Plusieurs acteurs appellent à la mise en œuvre de débats au sein de la société française portant sur les technologies de sécurité[2577]. L’ouverture de débats démocratiques portant sur les usages de technologies « augmentées » de sécurité publique, outre qu’elle permette une meilleure compréhension de leur fonctionnement, agit en faveur d'une transparence des procédures mises en œuvre par les autorités publiques. En ce sens, Axelle Lemaire souligne que les polémiques résultant des usages technologiques par les forces de l’ordre reposent sur « l’incompréhension entre l’administration française et les citoyens, et l’absence de débats politiques en amont »[2578]. Elle ajoute déplorer que « dans le contexte des menaces de sécurité qui pèsent sur notre pays, les termes d’un débat de qualité, favorisant l’émergence de l’acceptabilité sociale, ne sont jamais posés »[2579]. De même, l’organisation d'un débat public par la CNIL concernant les enjeux relatifs aux algorithmes et aux outils d'IA en décembre 2017 a suscité l’intérêt de nombreux acteurs[2580]. Les résumés des débats ont ainsi permis de formuler deux grands principes pour régir leurs usages : la loyauté et la vigilance[2581].

874. Le mode participatif dans le cadre d'un débat public permettrait d'informer les citoyens sur l'emploi des techniques de surveillance « augmentées », les apports attendus et les conséquences notamment quant aux restrictions aux droits et libertés en vue de concilier les intérêts des différentes parties prenantes[2582]. Ce mode participatif repose sur une implication directe des citoyens au processus de « conception, de mise en œuvre et d’évaluation des politiques

---

2577 Voir notamment : Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 82 ; Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, pp. 52-54 ; CNIL, « La CNIL appelle à la tenue d’un débat démocratique sur les nouveaux usages des caméras vidéo », *op. cit.*

2578 AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, Préface d’Axelle Lemaire, p. 11.

2579 *Idem*, p. 12.

2580 CNIL, Rapport de synthèse du débat public animé par la CNIL sur les enjeux éthiques des algorithmes et de l'intelligence artificielle « Comment permettre à l’Homme de garder la main ? - Rapport sur les enjeux éthiques des algorithmes et de l’intelligence artificielle », *op. cit.*

2581 *Idem*, spéc. pp. 48-50.

2582 Sénat, Rapport d'information n° 627 (2021-2022) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », *op. cit.*, p. 82.

publiques »[2583]. Il favorise l'acceptabilité des technologies par l'intermédiaire d'une pratique de transparence de leurs usages par les autorités publiques. Néanmoins, les bénéfices qui pourraient résulter de ces débats reposent sur un encadrement de ceux-ci par des représentants de la société civile et des membres de la communauté scientifique[2584]. Par ailleurs, le recours à des dispositions législatives expérimentales en matière de technologies « augmentées » de sécurité publique permet d'ouvrir le débat et de déterminer de manière concrète les attentes des citoyens. La mise en œuvre d'un mode de participation en ligne (sur le modèle de la loi pour une République numérique[2585]) serait susceptible de convenir au mode participatif entourant l'usage de ces technologies[2586]. Enfin, les membres de la communauté scientifique constituent un ensemble d'acteurs majeurs à la compréhension des enjeux et pourraient contribuer à la mise en œuvre des débats publics en soumettant des recommandations quant aux usages possibles au regard de l'état de l'art ainsi qu'aux progrès encore attendus en la matière.

875. Le renouvellement du concept de proportionnalité, qui pourrait être appliqué aux technologies « augmentées », consisterait donc à intégrer des moyens d'information et d'échange entre toutes les parties prenantes. Le Conseil d'État estime en ce sens que l'enjeu principal concernant le recours à des technologies « augmentées » repose essentiellement sur « la capacité individuelle de chacun, et plus encore la capacité collective du corps social, à les penser et à en maîtriser le processus »[2587]. Dans le même sens, certains auteurs considèrent, s'agissant du recours à ces technologies, qu'une solution valable aux problématiques qu'elles engendrent se situe davantage dans le fait « de redonner à toutes les parties prenantes un pouvoir, une visibilité et une capacité d'agir sur les décisions »[2588]. Ils insistent ainsi sur le besoin de rééquilibrer les pouvoirs des différentes parties prenantes, qu'il s'agisse des personnes concernées par les décisions pouvant porter atteinte à leurs droits et libertés mais aussi, dans le cadre d'un usage de sécurité publique, des

---

2583 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 52.

2584 *Ibid*.

2585 Plateforme mise à la disposition des français afin qu'ils contribuent à l'élaboration du projet de loi pour une République numérique [en ligne].

2586 Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 53.

2587 CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », *op. cit.*, p. 101.

2588 DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, *op. cit.*, p. 255.

forces de l'ordre et des services de secours[2589]. En d'autres termes, le recours proportionné aux technologies « augmentées » repose sur une transparence de leurs usages et une compréhension globale de leur mode de fonctionnement qui requièrent une implication de tous. Ce n'est que dans cette perspective que les technologies de surveillance « augmentées » de sécurité publique, telles que les drones aériens, pourront assurer une conciliation effective entre les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions, d'une part, et des droits et libertés, d'autre part.

[2589] *Idem*, p. 256.

CONCLUSION DU TITRE II

876. Les technologies de surveillance « augmentées » de sécurité publique suscitent autant d'intérêts que de doutes. Afin d'assurer le contrôle de leur utilisation et de favoriser leur acceptabilité sociétale, plusieurs mesures juridiques, techniques et organisationnelles doivent être mises en œuvre. Ces mesures reposent essentiellement sur quatre piliers que sont l'adéquation à un cadre juridique et une mise en débat du recours à ces technologies, la réalisation d'études d'impact, une conception responsable, et une évaluation continue intégrant éventuellement une procédure de certification. Aussi, dans la perspective des décisions qui seront prises à l'aide d'un SIA par les forces de l'ordre, la mise en œuvre du droit au recours effectif pour les personnes concernées s'avère capital en vue de garantir l'exercice de leurs droits et libertés. Le recours à des technologies « augmentées » nécessite un effort collectif dès leur conception. Par ailleurs, selon les finalités de ces technologies et le type de données qu'elles collectent, l'adoption de dispositions adaptées au cas par cas, précédée par un cadre juridique expérimental, semble davantage convenir pour assurer une protection effective des droits et libertés.

877. Indépendamment de l'adoption de mesures spécifiquement prévues à l'usage des technologies « augmentées », leur mise en œuvre nécessite un renforcement général du contrôle de proportionnalité des dispositions et mesures adoptées pour autoriser leur usage. Les drones aériens « augmentés » de sécurité publique, du fait de l'intégration d'outils algorithmiques d'analyse d'images, changent la nature de la surveillance de la voie publique et requièrent un contrôle de proportionnalité approfondi de la part des organes juridictionnels, à commencer par le Conseil constitutionnel. Ce dernier aura déjà eu à contrôler des dispositions portant sur ces technologies mais uniquement dans le cadre de leur usage à titre expérimental. Or, la variabilité de son contrôle de proportionnalité concernant les dispositifs à l'usage de la sécurité publique ne permet pas d'assurer une garantie effective des droits et libertés faisant l'objet de restrictions. Dès lors, il apparait nécessaire de repenser le principe de proportionnalité en ouvrant le débat aux citoyens dans le cadre du processus de détermination des usages de ces outils de surveillance.

CONCLUSION DE LA DEUXIÈME PARTIE

878. Depuis la tragédie des attentats du 11 septembre 2001, le constat est fait d'un affaiblissement des garanties des droits et libertés à l'instar du droit à la sûreté qui, réaffirmé sous les traits de la liberté individuelle, a vu son champ se réduire afin de mieux se plier aux exigences de l'ordre public sous la pression des politiques sécuritaires. En ce sens, ces dernières ont œuvré à l'introduction du concept de sécurité qu'elles s'efforcent d'ériger en droit fondamental faisant ainsi de la restriction aux libertés le principe plutôt que l'exception. Face à cela, les juridictions internes se révèlent parfois impuissantes à enrayer le mécanisme consistant à recourir à des technologies toujours plus intrusives à des fins de lutte contre l'insécurité. Le Conseil constitutionnel fait ainsi souvent preuve d'une certaine souplesse à l'égard du législateur lors du contrôle des textes introduisant de nouvelles mesures ou de nouveaux moyens à l'usage de la sécurité publique. Dès lors, les juridictions internes peinent à garantir de manière effective les droits et libertés. Cependant, les juridictions européennes se montrent davantage protectrices de ceux-ci notamment concernant les technologies utilisées à des fins de traitement de DACP, y compris au moyen d'algorithmes d'IA, par les forces de l'ordre. Enfin, la CNIL joue un rôle primordial de garant des droits et libertés pour faire face à ces technologies.

879. Les missions de la CNIL devraient, en ce sens, s'amplifier avec l'arrivée du REIA. Le texte européen s'inscrit dans la continuité du RGPD en regroupant un ensemble de principes communs particulièrement protecteurs des droits et libertés. En outre, ce texte insiste sur la mise en œuvre de mesures tant juridiques que techniques allant de la conception à l'utilisation de technologies reposant sur l'IA et sur la dimension multidisciplinaire du sujet permettant de prendre en compte tous les aspects nécessaires à la protection effective des droits et libertés. En France, la position du Parlement en faveur d'une législation expérimentale, au cas par cas, visant à évaluer le caractère adapté et nécessaire d'une technologie « augmentée » est salutaire en satisfaisant deux des critères du contrôle de proportionnalité auquel les juridictions supranationales et nationales recourent fréquemment pour garantir l'exercice des droits et libertés. Néanmoins, il apparait que ce contrôle de proportionnalité mériterait d'être davantage systématisé au sein de la jurisprudence et que le principe sur lequel il repose nécessite d'être repensé afin d'impliquer les citoyens dans la définition des usages des technologies « augmentées » telles que les drones aériens « augmentés » de sécurité publique.

CONCLUSION GÉNÉRALE

880. La révolution numérique est porteuse d'opportunités d'amélioration des missions de sécurité publique. Les drones aériens « augmentés » sont une illustration des promesses apportées par les développements technologiques. Pour autant, leurs performances en matière de traitement des données ne peuvent aider à assurer une meilleure protection des individus que dans la mesure où ces technologies garantissent dans le même temps le maintien des droits et libertés sur lesquels repose l'État de droit.

881. Une transformation du rapport sûreté-sécurité - Ainsi, les drones aériens « augmentés » de sécurité publique s'insèrent dans le rapport, en perpétuel renouvellement, entre la sûreté et la sécurité. L'introduction des dispositifs de surveillance de la voie publique a contribué à l'évolution de ce rapport qui, influencé par une politique sécuritaire, a progressivement basculé d'une domination de la sûreté, comme principe de l'État de droit, à celui de sécurité, comme concept dégagé indirectement de la notion d'ordre public. Ce basculement de la sûreté vers la sécurité, loin de n'être qu'un glissement sémantique, a permis d'introduire l'idée d'un droit fondamental à la sécurité et est devenu le symbole d'une quête constante de lutte contre l'insécurité. Pourtant, la professeure Danièle Lochak affirmait avec raison qu' « à vouloir traquer toutes les illégalités et instaurer une transparence intégrale en éradiquant le secret qui entoure les comportements individuels, on se dirige inéluctablement vers une société policière, voire totalitaire »[2590] dans laquelle les droits et libertés ne seraient plus le principe.

882. Une massification des outils de surveillance de la voie publique - L'évolution du rapport favorisant la sécurité plutôt que la sûreté se reflète au travers de la multiplication des dispositifs policiers qui reposent, pour une grande part, sur des outils technologiques toujours plus intrusifs. L'étude de l'évolution des dispositifs de surveillance de la voie publique a souligné les défaillances de cette politique sécuritaire par une absence de démonstration de la contribution effective de ces technologies à remplir les objectifs de valeur constitutionnelle de sauvegarde de l'ordre public et de recherche des auteurs d'infractions. Pour le professeur Guillaume Desgens-Pasanau, le recours inlassable à de nouveaux systèmes de vidéoprotection et l'introduction de

[2590] LOCHAK (D.), « La dénonciation, stade suprême ou perversion de la démocratie ? » *in L'État de droit. Mélanges en l'honneur de Guy Braibant*, Paris, Dalloz, 1996, 817 p., p. 467.

nouvelles dispositions permettant d'assurer leur encadrement sont « symptomatique[s] de ce processus irréversible appelé "effet de cliquet" [où] une fois qu'une technologie de surveillance est mise en œuvre, son développement devient inéluctable et s'inscrit dans des usages de plus en plus banalisés à mesure qu'ils sont socialement acceptés »[2591].

883. Par ailleurs, l'implication du secteur privé dans les activités de sécurité publique en matière de vidéoprotection avait déjà entamé le débat sur le terrain de la délégation de pouvoirs de police. L'étude de la jurisprudence administrative et constitutionnelle a permis d'éclaircir la question en qualifiant ces usages de délégation de missions de police, permettant ainsi à l'autorité publique de conserver la compétence exclusive du pouvoir décisionnel. Cependant, l'introduction des technologies « augmentées » d'aide à la prise de décision en matière de police est venue rebattre les cartes. Si toutefois la décision demeure, en théorie, entre les mains des forces de l'ordre, plusieurs études ont démontré les possibilités de biais d'ancrage ou de biais d'automatisation[2592] qualifiant l'influence que peuvent avoir ces technologies, conçues par des entreprises privées, sur le raisonnement des utilisateurs. Il est donc possible d'imaginer qu'une part du pouvoir des activités de police, propre au régalien, pourrait être en partie déléguée au secteur privé par l'intermédiaire des algorithmes d'aide à la prise de décisions à l'usage de la sécurité publique.

884. Les finalités multiples d'utilisation des drones aériens qu'autorise la loi RPSI permettent d'augmenter considérablement les possibilités de traitement de DACP et, par voie de conséquence, les atteintes au droit à la vie privée et à la protection des DACP ou encore à la liberté d'aller et venir. En outre, leur association à des algorithmes d'analyse d'images à des fins de collecte de preuves des infractions suscite une inquiétude légitime en termes de respect des droits de la défense, compte tenu de l'absence de démonstration de leur fiabilité et de l'opacité qui entoure leur fonctionnement. Il est ainsi possible de craindre une atteinte aux principes du contradictoire et de la présomption d'innocence qui permettent pourtant d'assurer l'équilibre entre les parties au procès pénal. Les drones aériens « augmentés » de sécurité publique mettraient dès lors en péril la liberté individuelle et plus encore le droit à la sûreté, auquel elle est assimilée, qui excluait également toute

---

[2591] DESGENS-PASANAU (G.), « Traçage des données mobiles : ne sacrifions pas la protection de nos données sur l'autel de la crise sanitaire », *JCP G* n°18, 4 mai 2020, 543. Voir aussi en ce sens : Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), *op. cit.*, p. 38.

[2592] Voir pour rappel : CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022, *op. cit.*, p. 104.

forme d'accusation arbitraire.

885. L'étude de la jurisprudence nationale a permis de démontrer l'insuffisance des garanties offertes par les voies juridictionnelles internes, confrontées à la pression des politiques sécuritaires qui cherchent à mettre en œuvre des technologies toujours plus intrusives et parfois mal maîtrisées. Si toutefois les juridictions européennes contribuent davantage à la protection des droits et libertés à l'ère du « tout numérique », cette protection est retardée par leur saisine après épuisement des voies de recours internes, d'une part, et limitée par leur tendance à laisser une large marge d'appréciation aux États en matière policière, d'autre part. Bien que les voies juridictionnelles demeurent un facteur assurant la garantie des droits et libertés, elles ne sont plus seules à agir aujourd'hui en ce sens et sont généralement associées aux autorités non-juridictionnelles dont les mécanismes de protection ont déjà fait leur preuve, telles que la CNIL et l'ANSSI s'agissant des usages technologiques. Leur statut de « nouveaux » garants des droits et libertés ne suffira pas cependant pour faire face à l'introduction des technologies « augmentées » à des fins de sécurité publique.

886. Reprendre la main sur les dispositifs de surveillance de la voie publique - Dès lors, l'introduction des technologies de surveillance « augmentées » sur la voie publique exige une réadaptation du cadre juridique existant afin de prendre en considération toutes leurs potentialités d'amélioration de la sécurité publique, d'une part, et d'atteintes aux droits et libertés, d'autre part. Les dispositions du REIA s'avèrent en ce sens prometteuses, apportant un cadre général aux États membres de l'Union européenne. Elles se révèlent également plus strictes que celles du RGPD ou de la DPJ, qui autorisaient sous conditions le traitement de DACP quand le REIA introduit des interdictions concernant certains types de traitement de données par des logiciels d'IA que les autorités européennes jugent trop attentatoires aux droits et libertés. Aussi, la volonté du législateur national de mettre en œuvre un cadre expérimental pour chaque nouvelle technologie « augmentée » à l'usage des forces de l'ordre, afin de juger de leur efficacité concrète et de leur acceptabilité avant toute pérennisation éventuelle, constitue un gage de protection des droits et libertés tout en ne bridant pas l'innovation.

887. Le renouvellement des usages technologiques des forces de l'ordre nécessite un contrôle de la puissance publique qui implique notamment l'application du principe de souveraineté dès la conception de ces outils afin de ne pas laisser aux entreprises étrangères le soin de définir leurs

modes d'utilisation[2593]. Aussi, ces évolutions technologiques requièrent un renouvellement de l'approche de la sécurité publique qui tiendrait davantage compte des cybermenaces pesant sur toute technologie, de la formation des agents à leur usage spécifique, et des recommandations formulées par les membres de la communauté scientifique.

888. La transparence, un principe cardinal à l'emploi de technologies « augmentées » de sécurité publique - Cette étude aura permis de révéler que l'opacité des technologies de surveillance « augmentées » engendre des potentialités d'atteintes considérables aux droits et libertés dans la mesure où elle ne permet pas aux acteurs d'en assurer le contrôle, d'une part, et qu'elle affaiblit les possibilités pour les personnes concernées par le traitement de DACP de faire garantir leurs droits, d'autre part[2594]. Dès lors, la transparence et l'explicabilité de ces technologies constituent une étape essentielle à la sauvegarde des droits et libertés. À cette fin, la conception et l'encadrement des usages de ces technologies doivent impliquer un ensemble pluridisciplinaire d'acteurs en vue de prendre en considération tous les aspects nécessaires aux fins de garantir la protection des droits et libertés. En outre, le respect des principes démocratiques propres à l'État de droit requière, plus que jamais à l'heure des technologies de surveillance « augmentées », une participation du public dans le choix à opérer en matière d'outils numériques utilisés à des fins de sécurité publique. Cela permettrait de prendre davantage en considération les aspects sociétaux sans pour autant sacrifier les droits et libertés individuels. Dès lors, la législation entourant les technologies de sécurité publique gagnerait à s'inspirer du mode de participation mis en œuvre lors de l'élaboration de la loi pour une République numérique[2595].

889. Le renforcement d'un usage proportionné des technologies de surveillance de sécurité publique - L'analyse de la jurisprudence nationale et européenne révèle autant les apports que la fragilité du contrôle de proportionnalité qu'assurent aujourd'hui les différentes juridictions en matière d'usages technologiques par les forces de l'ordre. Pourtant, en matière de recours à des technologies de traitement de DACP, la garantie des droits et libertés repose sur le respect du

---

[2593] AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, *op. cit.*, Préface d'Axelle Lemaire, p. 13.

[2594] JEAN (A.), *Les algorithmes font-ils la loi ?*, *op. cit.*, p. 25 : En ce sens, « la justice exige une transparence inconditionnelle pour permettre une appréciation juste de la loi, et une décision judiciaire lisible et compréhensible par tous ».

[2595] Le Gouvernement avait mis en œuvre une plateforme permettant aux français de contribuer à l'élaboration du projet de loi pour une République numérique [en ligne] qui fut finalement promulguée le 7 octobre 2016 (Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *op. cit.*)

principe de proportionnalité qui se reflète au travers des dispositions de la règlementation relative à la protection des données. L'usage de technologies « augmentées » par les forces de l'ordre ne doit pas mener à ce que Yannick Meneceur appelle la « mécanique totalitaire », qui consisterait à faire reposer les objectifs de sauvegarde de l'ordre public et de recherche des auteurs d'infractions sur « des calculs algorithmiques en temps réel et des dispositifs généralisés de surveillance, sans aucun angle mort »[2596]. Il convient dès lors de renforcer l'application du principe de proportionnalité dans la mise en œuvre des technologies « augmentées » de sécurité publique en limitant leur usage ainsi que les données traitées à ce qui est strictement nécessaire. L'arrivée des drones aériens « augmentés » de sécurité publique doit donc s'accompagner d'un renouvellement des garanties des droits et libertés, afin de ne pas contribuer au déséquilibre du rapport entre sûreté et sécurité.

[2596] MENECEUR (Y.), *L'Intelligence artificielle en procès*, *op. cit.*, p. 400.

ANNEXES

Annexe 1 Petite histoire des drones aériens

890. Les drones aériens faisaient autrefois seulement l'objet de romans ou de films de science-fiction. Aujourd'hui, ils ont quitté le monde de l'imaginaire et dépassé le seul cadre d'une utilisation à des fins militaires. Ils ont désormais intégré notre quotidien que ce soit dans le cadre d'une livraison, de la surveillance d'une foule lors d'un grand rassemblement et…demain du transport. Leur histoire a débuté il a un siècle puisque dès la première Guerre mondiale, des chercheurs au service des armées commencent à développer des aéronefs sans pilote téléguidés[2597]. En France, le capitaine Max Boucher, pilote du service de l'aéronautique, effectua les premiers essais de pilotage d'un avion télécommandé[2598], le 2 juillet 1917. Cet avion télécommandé *Voisin,* équipé du système *Détable*, parvient à voler sans intervention humaine sur un kilomètre. Malheureusement, les expériences furent rapidement écourtées par peur des risques encourus. Passant outre l'interdiction du Gouvernement, Max Boucher poursuivra ses expériences et parviendra le 14 septembre 1918 à télépiloter ce même type d'avion sur 100 kilomètres. En 1924, le projet aboutit à deux prototypes : « l'avion semi-automatique et l'avion sans pilote »[2599] qui seront par la suite acquis par le ministère de la guerre et constituent la naissance des premiers prototypes de drones militaires. Les expériences seront ensuite reprises par le Service technique aéronautique (STAé) mais les projets d'aéronefs sans pilote seront finalement abandonnés au profit du pilotage automatique.

891. Les projets d'aéronefs sans pilote à bord ne réapparaitront finalement qu'après la Seconde guerre mondiale. Considérant le nombre de pertes d'avions d'observation, la nécessité d'élaborer des avions militaires sans pilote à bord redevient un sujet d'étude. Vers la fin des années 1950, la France transformera un avion de chasse à réaction, le *Mistral*, en drone aérien[2600]. Par cette transformation, l'aéronef fit office de cible d'entrainement pour la défense aérienne. Cependant, les expérimentateurs firent face aux problèmes de liaison radio permettant de contrôler l'aéronef. Afin d'assurer l'intégrité physique des personnes au sol, un avion de chasse était systématiquement

---

[2597] ZUBELDIA (O.), *Histoire des drones : de 1914 à nos jours*, Paris Perrin, 2012.

[2598] MERCIER (D.), *Les drones aériens : passé, présent et avenir. Approche globale*, Paris, La Documentation Française, coll. Stratégie aérospatiale, 2013, 706 p., pp.39-63 ; MONNIER (E.), « Un premier drone militaire décolle en France », *Science et Vie* n°1198, juillet 2017, pp. 128-130.

[2599] MERCIER (D.), *Les drones aériens : passé, présent et avenir. Approche globale*, *op. cit.*

[2600] BROCAREL (A.), « L'insertion et la circulation des drones militaires, p. 82 *in* EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, *op. cit.*

envoyé préalablement au décollage du drone aérien permettant de l'abattre en cas de perte de contrôle des commandes. Les drones aériens furent de nouveau utilisés en France dans les années 1960, « tel le R 20 de Nord-Aviation, dérivé de l'engin cible CT 20 »[2601]. Les premiers drones d'observation seront également utilisés au cours de cette même période.

892. Par la suite, la recherche et les expériences en matière de drones aériens se sont peu à peu développées au niveau mondial. Les États-Unis ont été les premiers à recourir fréquemment à des drones militaires dès la guerre du Vietnam. Ils ont ensuite transmis leurs compétences de cette technologie à l'État d'Israël qui commença à les utiliser lors de la guerre de Kippour en 1973 et les enrichira en les équipant de caméras filmant en temps réel. En Europe, ce n'est que lors des conflits de la guerre du Golfe que les Britanniques et les Français commencèrent également à se servir des drones aériens. Aujourd'hui, les États-Unis et l'État d'Israël sont reconnus comme étant les deux puissances militaires les plus à la pointe au niveau mondial en matière de drones aériens de surveillance[2602].

[2601] ONERA, « Mieux connaître les drones », 48 p. [en ligne] consulté le 6 juillet 2017.

[2602] PFLIMLIN (E.), *Drones et robots. La guerre des futurs*, Levallois-Perret, Studyrama, 2017, pp. 64-65.

Annexe 2 Résumé des travaux sur le projet FUI-COOPOL

893. Les capacités dont peuvent faire preuve les drones aériens n'ont pas échappé aux agents de forces de l'ordre et des services de secours. Cette appétence pour les drones aériens a participé à l'élaboration de nombreux projets dont un projet (financé par le Fond unitaire interministériel (FUI)) intitulé « COOPOL » (Capacité d'appui aux Opérations de secOurs et POLice) qui visait à mettre à disposition des sapeurs-pompiers, des forces de police et de la gendarmerie nationales un système multi-drones de secours en milieu urbain et d'aide au maintien de l'ordre[2603]. Le projet, qui a pris fin en septembre 2020, comprenait parmi ses développements la détection de mouvements de foule, la reconnaissance de zone, la modélisation 3D de l'intérieur d'un bâtiment, l'assistance aux personnes lors des interventions d'urgence, mais aussi le suivi et la réidentification de personnes dans le cadre de la poursuite d'un suspect[2604].

894. Les drones aériens développés par le projet COOPOL reposaient sur un objectif d'aide aux missions de sécurité publique et à la surveillance des zones impliquées lors des missions qu'il s'agisse d'un incendie, de la surveillance d'un évènement à des fins de lutte contre les troubles à l'ordre public ou encore de la poursuite d'un individu ayant potentiellement commis une infraction. Le projet a donné lieu à deux études juridiques : l'une effectuant un état de l'art de la réglementation, l'autre analysant l'incidence du recours à ces technologies sur les droits et libertés. L'étude réglementaire a permis de révéler les verrous juridiques subsistants (notamment en matière de réglementation portant sur les algorithmes) ainsi que le manque de clarté du cadre juridique applicable à l'emploi de drones aériens de sécurité publique compte tenu notamment de la disparité des dispositions au sein des différents codes. L'étude des enjeux juridiques entendait sensibiliser les acteurs (concepteurs et utilisateurs) quant aux conséquences sur le comportement des personnes ainsi que sur l'exercice de leurs droits et libertés, en particulier de leur droit à la vie privée, que pouvaient avoir les drones aériens « augmentés » de sécurité publique. Une étude des aspects sociologiques a également mis en lumière « l'état de conscience » du public (professionnels et non professionnels du secteur de la sécurité intérieure) s'agissant des usages technologiques par les forces de l'ordre et les services de secours.

[2603] Voir pour d'autres informations le site du projet [en ligne].

[2604] COOPOL, « Compte rendu de la réunion de lancement », 7 novembre 2016, p. 13 (réf. COOPOOL_D051_CR_Réunion de lancement_20161107).

Annexe 3 Lois nationales relatives à la sécurité publique/intérieure

Liste des lois relatives à la sécurité adoptées depuis les attentats du 11 septembre 2001[2605] :

- Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure ;
- Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement ;
- Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés ;
- Loi n° 2018-697 du 3 août 2018 relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique ;
- Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme ;
- Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique ;
- Loi n° 2016-339 du 22 mars 2016 relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs ;
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement ;
- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale ;
- Loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme ;
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure ;
- Loi n° 2008-1245 du 1er décembre 2008 visant à prolonger l'application des articles 3,6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ;
- Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ;
- Loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile ;
- Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure ;
- Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure ;
- Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

[2605] Liste inspirée de VIDAL-NAQUET (A.), « « La sécurité en droit constitutionnel : non-dit ou non-être ? » *in* NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, *op. cit.*, p. 82 et mise à jour des dernières lois en matière de sécurité intérieure.

BIBLIOGRAPHIE

I. Ouvrages généraux, dictionnaires, manuels et traités

ANDRIANTSIMBAZOVINA (J.) *et al.*, *Dictionnaire des droits de l'homme*, Paris, PUF, coll. Quadrige, 2008, 1120 p.

ALLAND (D.) et RIALS (R.) (dir.), *Dictionnaire de la culture juridique*, Paris, PUF, 6ème édition, 2019, 1696 p.

BERTRAND-MIRKOVIC (A.), *Droit civil - personnes, famille*, Paris, éditions Studyrama, 4e édition, 2014, 495 p.

BIOY (X.), *Droits fondamentaux et libertés publiques*, Paris, LGDJ, coll. Cours, 7ème édition, 2022, 1010 p.

BIOY (X.), BURGORGUE-LARSEN (L.), DEUMIER (P.), DREYER (E.), DUPRÉ DE BOULOIS (X.), MARTINON (A.) et TINIÈRE (R.), *Les grands arrêts du droit des libertés fondamentales*, Paris, Dalloz, 3ème édition, 2021, 943 p.

BOULOC (B.), *Droit pénal général,* Paris, Dalloz, coll. Précis droit privé, 23ème édition, 2013, 950 p.

BURDEAU (G.), *Libertés publiques,* Paris, LGDJ, 4ème édition, 1972, 458 p.

BURDEAU (G.), *Traité de science politique*, Tome I, vol. 1, Paris, LGDJ, 3ème édition, 1980, 483 p.

CARBONNIER (J.), *Droit civil*, vol. 1, Paris, PUF, 2004, 2574 p.

CHAGNOLLAUD (D.) et DRAGO (G.), *Dictionnaire des droits fondamentaux*, Paris, Dalloz, 2010, 751 p.

CHAPUS (R.), *Droit administratif général*, Tome I, LGDJ, coll. Précis Domat, 15ème édition, 2001, 1440 p.

CORNU (G.) (dir.), *Vocabulaire juridique*, Paris, PUF, coll. Quadrige, 13ème édition, 2020, 1091 p.

DENIZEAU (C.), *Droit des libertés fondamentales*, Paris, Éditions Vuibert, 10ème édition, 2021, 448 p.

DUGUIT (L.), *Traité de droit constitutionnel - Les libertés publiques*, Tome V, (1925), Paris, Hachette, 2ème édition, 1981, 716 p.

DUMONT (G.) et SIRINELLI (J.), *Droit administratif*, Paris, Dalloz, 14ème édition, 2021, 690 p.

DUPRÉ DE BOULOIS (X.), *Droit des libertés fondamentales*, Paris, PUF, 2ème édition, 2020, 587 p.

ESMEIN (A.), *Éléments de droit constitutionnel français et comparé*, Paris, Sirey, tome I, 8ème édition, 1286 p.

FAVOREU (L.) *et al.*, *Droit constitutionnel*, Paris, Dalloz, coll. Précis, 24ème édition, 2021, 1200 p.

FAVOREU (L.) *et al.*, *Droit des libertés fondamentales*, Paris, Dalloz, coll. Précis, 8ème édition, 2021, 978 p.

FAVOREU (L.) et PHILIP (L.), *Les grandes décisions du Conseil constitutionnel*, Paris, Dalloz, 20ème édition, 2022, 1128 p.

GAUDEMET (Y.), *Droit administratif*, Paris, LGDJ, 23ème édition, 2020, 648 p.

GAUTHIER (C.), PLATON (S.) et SZYMCZAK (D.), *Droit européen des droits de l'homme*, Paris, Sirey, 2016, 518 p.

GUINCHARD (V. S.) et BUISSON (J.), *Procédure pénale*, Paris, LexisNexis, 15e édition, 2022, 1620 p.

HAURIOU (M.), *Précis de droit administratif et de droit public* [1933], Paris, Sirey, 12ème édition, 2003, 1150 p.

HENNETTE-VAUCHEZ (S.) et ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, Paris, Dalloz, 4ème édition, 2020, 775 p.

JAUME (L.), *La Déclaration des droits de l'homme et du citoyen, du débat 1789-1793 au Préambule de 1946*, Paris, Flammarion, 1989, 376 p.

LATOUR (X.) et PAUVERT (B.), *Manuel de libertés publiques et droits fondamentaux*, Levallois-Perret, édition Studyrama, 9ème édition, 2021, 457 p.

LEBRETON (G.), *Libertés publiques et droits de l'homme*, Paris, Sirey, 8ème édition, 2008, 570 p.

LÉCUYER (Y.) et LEMAIRE (F.), *Cours de droits humains et libertés*, Paris, édition Gualino, 2022, 690 p.

LOCHAK (D.), *Les droits de l'homme*, Paris, La Découverte, coll. Repères, 4ème édition, 2018, 128 p.

OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, Paris, LGDJ, 7ème édition, 2019, 732 p.

ODENT (R.), *Contentieux administratif*, Tome II, Paris, Dalloz, 2007, 783 p.

PETIT (J.) et FRIER (P-L.), *Droit administratif*, Paris, LGDJ, 2022, 812 p.

PLESSIX (B.), *Droit administratif général*, Paris, LexisNexis, 3ème édition, 2020, 1742 p.

RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome I, Paris, PUF, 9ème édition, 2003, 271 p.

RIVERO (J.) et MOUTOUH (H.), *Les libertés publiques*, Tome II, Paris, PUF, 7ème édition, 2003, 269 p.

ROBERT (J.) et DUFFAR (J.), *Droits de l'homme et libertés fondamentales*, Paris, Montchrestien, 8ème édition, 2009, 908 p.

ROUSSEAU (D.), GAHDOUN (P-Y.) et BONNET (J.), *Droit du contentieux constitutionnel*, Paris, LGDJ, 12ème édition, 2020, 1039 p.

ROUSSEL (G.) et ROUX-DEMARE (F-X.), *Procédure pénale*, Paris, Vuibert, 12ème édition, 2021, 480 p.

ROUVILLOIS (F.), *Droit constitutionnel - 1. Fondements et pratiques*, Paris, Flammarion, coll. Champs-Université, 5ème édition, 2001, 435 p.

ROUVILLOIS (F.), *Libertés fondamentales*, Paris, Flammarion, coll. Champs-Université, 2ème édition, 2016, 446 p.

SUDRE (F.), *Droit européen et international des droits de l'homme*, Paris, PUF, 15ème édition, 2021, 1044 p.

SUDRE (F.), *La convention européenne des droits de l'Homme*, Paris, PUF, coll. Que sais-je ?, 11ème édition, 2021, 125 p.

TRUCHET (D.), *Droit administratif*, Paris, PUF, 9ème édition, 2021, 564 p.

TRUCHET (D.), *Le droit public*, Paris, PUF, coll. Que Sais-je ?, 2018, 128 p.

VERGÈS (É.), *Procédure pénale*, Paris, LexisNexis, 6ème édition, 2020, 388 p.

WACHSMANN (P.), *Libertés publiques*, Paris, Dalloz, 9ème édition, 2021, 1033 p.

II. Ouvrages spéciaux, mélanges et thèses

Association française pour la recherche en droit administratif, *Les controverses en droit administratif*, Paris, Dalloz, 2017, 240 p.

L'État de droit. Mélanges en l'honneur de Guy Braibant, Paris, Dalloz, 1996, 817 p.

Mélanges offerts à Marcel WALINE, Le juge et le droit public, Paris, LGDJ, Tome II, 1974, 858 p.

Mélanges en l'honneur d'Yves Mayaud, Entre tradition et modernité : le droit pénal en contrepoint, Paris, Dalloz, 2017, 846 p.

Renouveau du droit constitutionnel. Mélanges en l'honneur de Louis Favoreu, Paris, Dalloz, 2007, 1783 p.

AFROUKH (M.), MAUBERNARD (C.) et VIAL (C.) (dir.), *La sécurité : mutations et incertitudes*, Paris, LGDJ, Institut Universitaire Varenne, coll. « Colloques & Essais », 2019, 232 p.

AÏM (O.), *Les Théories de la surveillance : Du panoptique aux Surveillance Studies*, Malakoff, Armand Colin, 2020, 253 p.

AMABILE (A.) et THODOROFF (B.), *Police numérique, une révolution sous surveillance ?*, Paris, Presses des Mines, 2020, 118 p.

ARMAND (G.), *L'autorité judiciaire, gardienne de la liberté individuelle dans la jurisprudence du Conseil constitutionnel*, Caen, Thèse, 2000.

ARPAGIAN, (N.), *La cybersécurité*, Paris, PUF, coll. Que sais-je, 2022, 128 p.

AUBY (J-B), *L'influence du droit européen sur les catégories du droit public*, Paris, Dalloz, 2010, 1006 p.

AUBY (J-B.) et DUTHEIL DE LA ROCHÈRE (J.) (dir), *Traité de droit administratif européen*, Bruxelles, Bruylant, 2ème édition, 2014, 1118 p.

AVOINE (G.) et KILLIJIAN (M-O.) (dir.), *13 défis de la cybersécurité*, Paris, CNRS Editions, 2020, 262 p.

AZOUAOU (P.), *L'indisponibilité des compétences en droit public interne*, Lyon, Mare & Martin, Thèse, 2016.

BASDEVANT (A.) et MIGNARD (J-P.), *L'empire des données - Essai sur la société, les algorithmes et la loi*, Paris, Édition Don Quichotte, 2018, 288 p.

BASEX (H.), MBANZOULOU (P.), RAZAC (O.) et ALVAREZ (J.) (dir.), *Les nouvelles figures de la dangerosité*, Paris, L'Harmattan, 2008, 402 p.

BAUER (A.) et FREYNET (F.), *Vidéosurveillance et vidéoprotection*, Paris, PUF, coll. « Que sais-je ? », 2012, 128 p.

BAUER (A.) et SOULLEZ (C.), *Les fichiers de police et de gendarmerie*, Paris, PUF, coll. « Que sais-je ? », 2ème édition, 2011, 128 p.

BAUER (A.) et VENTRE (A-M.), *Les polices en France*, Paris , PUF, coll. « Que sais-je ? », 2010, 128 p.

BEAUD (O.), *La puissance de l'État*, Paris, PUF, Léviathan, 1994, 512 p.

BEAULAC (L.), *La distinction police administrative - police judiciaire conserve-t-elle une utilité ?*, Université de Pau et des Pays de l'Adour, Thèse, 2001.

BELLIN (I.) et LABBÉ (S.), *Des Drones à Tout Faire ?: Ce Qu'ils Vont Changer Dans Ma Vie Au Quotidien*, Versailles, Editions Quae, 2016, 203 p.

BENSAMOUN (A.), *Les Robots : Objets scientifiques, objets de droits*, Lyon, Mare & Martin, 2016, 236 p.

BENSOUSSAN-BRULÉ (V.) et TORRES (C.), *Failles de sécurité et violation des données personnelles*, Bruxelles, éditions Larcier, coll. Manuels Larcier, 2016, 134 p.

BERNARD (P.), *La notion d'ordre public en droit administratif,* Paris, LGDJ, coll. Bibliothèque de droit public, Thèse, 1962, 291 p.

BIGO (D.) *et al.* (dir.), *Suspicion et exception*, Paris, L'Harmattan, 2008, 222 p.

BOILEAU (N.), *L'Art poétique*, 1872.

BUISSON (J.), *L'acte de police*, Lyon III, Thèse, 1988, 1237 p.

BURG (M.), *Droit fondamental et opérationnel du maintien de l'ordre public*, Nancy, PUN, coll. « Pour ainsi dire », 2020, 177 p.

CARBASSE (J-M.), *Histoire du droit pénal et de la justice criminelle*, Paris, PUF, 2000, 544 p.

CASSART (A.), *Droit des drones : Belgique, France, Luxembourg*, Bruxelles, éditions Bruylant, 2017, 187 p.

CHAMAYOU (G.), *Théorie du drone*, Paris, édition La Fabrique, 2013, 363 p.

CAMUS (C.), *La Guerre contre le terrorisme. Dérives sécuritaires et dilemme démocratique*, Paris, Éditions Le Félin, 2007, 151 p.

CARBASSE (J-M.), *Histoire du droit pénal et de la justice criminelle*, Paris, PUF, 2000, 445 p.

CHAPUS (R.), *L'administration et son juge*, Paris, PUF, 1999, 426 p.

CHARDEL (P-A.) (dir.), *Politiques sécuritaires et surveillance numérique*, Paris, CNRS Éditions, coll. les essentiels d'Hermès, 2014, 216 p.

CHEVALLIER-GOVERS (C.) (dir.), *L'échange de données dans l'Espace de liberté, de sécurité et de justice de l'Union européenne*, Mare & Martin, 2017, 545 p.

CLAMOUR (G.) et UBAUD-BERGERON (M.) (dir.), *Contrats publics. Mélanges en l'honneur du Professeur Guibal*, Montpellier, PUM, 2006, 1588 p.

CORRALES (M.), FENWICK (M.) and FORGÓ (N.) (Ed.), *Robotics, AI and the Future of Law*, Singapore, Springer, 2018, 237 p.

CUSTERS (B.), *The Future of Drone Use : Opportunities and Threats from Ethical and Legal Perspectives*, Den Haag, Editor T.M.C Asser Press, Springer, 2016, 386 p.

DANET (D.), HANON (J-P.) et BOISBOISSEL (G. de) (dir.), *La guerre robotisée*, Paris, édition Economica, 2012, 336 p.

DANTONEL-COR (N.) (dir.), *Les politiques publiques locales de sécurité intérieure*, Paris, L'Harmattan, 2015, 308 p.

DEBAETS (É.), DURANTHON (A.) et SZTULMAN (M.) (dir.), *Les fichiers de police*, Paris, LGDJ, Institut Universitaire Varenne, coll. Colloques & Essais, 2019, 425 p.

DE BELLESCIZE (R.), *Les services publics constitutionnels*, Paris, LGDJ, coll. Bibliothèque de droit public, Thèse, 2005, 486 p.

DE DAVID BEAUREGARD-BERTHIER (O.) et TALEB-KARLSSON (A.) (dir.), *Protection des données personnelles et Sécurité nationale : Quelles garanties juridiques dans l'utilisation du numérique ?,* Bruxelles, éditions Bruylant, 2017, 279 p.

DEFFRAINS (N.) et PLESSIX (B.), *Fichiers informatiques et sécurité publique*, Nancy, Presses Universitaires de Nancy, 2013, 241 p.

DELMAS-MARTY (M.), *Libertés et sûreté dans un monde dangereux*, Paris, Le Seuil, 2010, 274 p.

DELTORN (J-M) et PICHENOT (E.) (dir.), *Algorithmes et Société*, Paris, Éditions Archives contemporaines, 2021, 191 p.

DE MAISON ROUGE (O.), *Les cyberisques : La gestion juridique des risques à l'ère de l'immatérielle*, Paris, LexisNexis, 2018, 192 p.

DE MONTALIVET (P.), *Les objectifs de valeur constitutionnelle*, Paris, Dalloz, coll. « Bibliothèque parlementaire et constitutionnelle », Thèse, 2006, 702 p.

DESCHAUX-DUTARD (D.) et VIDELIN (J-C.) (dir.), *Annuaire du droit de la sécurité et de la défense 2020*, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, 2020, 252 p.

DESMOULIN-CANSELIER (S.) et LE MÉTAYER (D.), *Décider avec les algorithmes : quelle place pour l'Homme, quelle place pour le droit ?*, Paris, Dalloz, coll. Le sens du droit - Essai, 2020, 275 p.

DE STREEL (A.), et JACQUEMAIN (H.) (dir.), *L'intelligence artificielle et le droit*, Bruxelles, édition Larcier, 2017, 482 p.

DOARÉ (R.), DANET (D.) et BOISBOISSEL (G. de) (dir.), *Drones et killer robots : Faut-il les interdire ?*, Rennes, PUR, 2015, 267 p.

DOUILLET (A-C.), GERMAIN (S.), HELLEMAN (É.) et MELCHIOR (P.), *Vidéo-surveillance ou vidéo-protection ?*, Paris, Le Muscadier, coll. Le choc des idées, 2012, 127 p.

DUBREUIL (C-A) (dir.), *L'ordre public*, Paris, CUJAS, coll. Actes et Études, 2013, 342 p.

DUCASSÉ (P.), *Les techniques et le philosophe*, Paris, PUF, 1958, 176 p.

EDDAZI (F.) (dir.), *Le droit à l'épreuve des drones militaires*, Paris, LGDJ, coll. Grands colloques, 2018, 347 p.

ELIAS (N.), *La Dynamique de l'occident*, Paris, Édition Pocket, Évolution, 2003, 320 p.

ETCHEVERRY (P.), *Cyber et drones*, Paris, éditions Economica, 2018, 167 p.

EUBANKS (V.), *Automating inequalities. How High-tech tools profiles, police, and punish the Poor*, New-York, St. Martin's Press, 2018, 272 p.

FÉRAL-SCHUHL (C.), *Cyberdroit : Le droit à l'épreuve de l'internet*, Paris, Dalloz, 8e édition, 2020, 1888 p.

FOUCAULT (M.), *Surveiller et punir*, Paris, Gallimard, 1975, 318 p.

FOUCAULT (M.), *Sécurité, territoire, population*, Cours au Collège de France 1977-1978, Paris, Le Seuil, 2004.

GALLAIS (S.), *Cadre juridique de l'emploi des drones au combat*, Paris, Éditions L'Harmattan, 2013, 191 p.

GALLOIS (J.) et MUREL (R.) (dir.), *La sécurité globale. Perspectives juridiques & éthiques*, Paris, L'Épilogue, coll. L'unité du droit, 2022, 190 p.

GARRIDO (L.) (dir.), *Le droit à la sûreté : État des lieux, état du droit*, Paris, édition Cujas, 2012, 191 p.

GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, Paris, LGDJ, Thèse, 2014, 517 p.

GIUDICELLI-DELAGE (G.) et LAZERGES (C.) (dir.), *La dangerosité saisie par le droit pénal*, Paris, PUF, IRJS éditions, coll. Les voies du droit, 2011, 320 p.

GLEIZAL (J-J), *La police en France*, Paris, PUF, coll. Que sais-je ?, n° 2761, 1993, 128 p.

GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2021 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, vol. 6, 2021, 318 p.

GOHIN (O.) et LATOUR (X.) (dir.), *Annuaire 2022 Du droit de la sécurité et de la défens*e, Lyon, Mare & Martin, coll. Droit de la sécurité et de la défense, vol. 7, 2022, 316 p.

GORMAND (G.), *L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier*, Université Grenoble Alpes, Thèse, 2017.

GORRIEZ (F.), *Le droit de la cybersécurité*, Paris, Éditions Nuvis, 2019, 225 p.

GRANGER (M-A), *Constitution et sécurité intérieure : Essai de modélisation juridique*, Paris, LGDJ, Thèse, 2011, 493 p.

HAMBLING (D.), *Swarm Troopers : How small drones will conquer the world*, Archangel Ink Press, 2016, 322 p.

HELIE, *Traité d'instruction criminelle*, Tome IV, Plon, 2ème édition, 1886, 708 p.

HOANG (LN.) et EL MHAMDI (EM.), *Le fabuleux chantier : Rendre l'intelligence artificielle robuste ment bénéfique*, Paris, EDP sciences, 2019, 296 p.

JEAN (A.), *Les algorithmes font-ils la loi ?*, Paris, Éditions de l'Observatoire/Humensis, 2021, 215 p.

KEMPF (O.), *Introduction à la cyberstratégie*, Paris, éditions Economica, 2ème édition, 2015, 236 p.

KOLM (S. C.), *Justice and Equity*, MIT Press, 1998, 275 p.

KOSTA (E.), PIERSON (J.), SLAMANING (D.), FISCHER-HÜBNER (S.), KRENN (S.). *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Vienna, Springer International Publishing, August 20-24th 2018.

LAINGUI (A.) et LEBIGNE (A.), *Histoire du droit pénal : La procédure criminelle*, Tome II, Paris, Cujas, 1979, 158 p.

LAVENUE (J-J.) et VILLABA (B.), *Vidéosurveillance et détection automatique des comportements anormaux. Enjeux techniques et politiques*, Villeneuve d'Ascq, Presses universitaires du septentrion, 2011, 294 p.

LE CUN (Y.), *Quand la machine apprend*, Paris, Odile Jacob, 2019, 394 p.

LEMAIRE (É.), *L'oeil sécuritaire : Mythes et réalités de la vidéosurveillance*, Paris, La Découverte, 2019, 208 p.

LEONETTI (X.) et FÉRAL-SCHUHL (C.), *Cybersécurité, mode d'emploi*, PUF, 2022, 372 p.

LOBRY (A.), MÂZOUZ (A.) et WEIL (E.) (dir.), *Drones et droit*, Université de Cergy-Pontoise, coll. LEJEP, 2018, 183 p.

MALAURIE (P.), *Les contrats contraires à l'ordre public : Étude de droit civil comparé : France, Angleterre, URSS*, Reims, Éditions Matot-Braine, Thèse, 1953, 278 p.

MBONGO (P.) et LATOUR (X.) (dir.), *Sécurité, libertés et légistique : Autour du Code de la sécurité intérieure*, Paris, éditions L'Harmattan, 2012, 276 p.

MELLONI (D.), *Délégation de service public : du contrat à l'habilitation institutionnelle*, Nancy, Thèse, 2006.

MENECEUR (Y.), *L'Intelligence artificielle en procès*, Bruxelles, Bruylant, 2020, 434 p.

MERCIER (D.), *Les drones aériens : passé, présent et avenir. Approche globale*, Paris, La Documentation Française, coll. Stratégie aérospatiale, 2013, 706 p.

MORANGE (J.), *La déclaration des droits de l'homme et du citoyen*, Paris, PUF, coll. Que sais-je ?, 4ème édition, 2002, 128 p.

MORNET (M-N.), *La vidéosurveillance et la preuve,* Aix-Marseille, PUAM, Thèse, 2004, 347 p.

MOROZOV (E.), *Pour tout résoudre, cliquez ici. L'aberration du solutionnisme technologique*, Limoges, éditions FYP, 2014, 350 p.

MOUCHETTE (J.), *La magistrature d'influence des autorités administratives indépendantes*, Paris, LGDJ, Thèse, 2019, 714 p.

MUCCHIELLI (L.), *Vous êtes filmés : enquête sur le bluff de la vidéosurveillance*, Malakoff, Armand Collin, 2018, 222 p.

NGAMPIO-OBÉLÉ-BÉLÉ (U.) (dir.), *La sécurité en droit public*, Paris, LGDJ, Institut Universitaire Varenne, coll. « Colloques & Essais », 2018, 302 p.

N. GUIORA (A.), *Cybersecurity : Geopolitics, law, and policy,* New-York, Routledge, 2017.

NORRIS (C.) et MORAN (J.), *Surveillance, Closed Circuit Television and Social Control,* London, Routledge Edition, 1998, 304 p.

O'NEIL (C.), *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy*, New York, Crown Publishers, First edition, 2016, 209 p.

O'NEIL (C.), *Algorithmes, la bombe à retardement*, Paris, Éditions Les Arènes, 2018, 340 p.

PASQUALE (F.), *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, MA: Harvard University Press, 2015.

PAULIAT (H.), *La sécurité intérieure en Europe*, Limoges, PULIM, 2010, 231 p.

PELLÉ (S.) (dir.), *Quelles mutations pour la justice pénale du XXIe siècle ? À partir de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme de la justice*, Paris, Dalloz, coll. Thèmes et commentaires, 2020, 296 p.

PERERA (S.), *Le principe de liberté en droit public français*, Paris, LGDJ, Thèse, 2021, 606 p.

PERRIER (M.), *Le recours au contrat en matière de police administrative*, Thèse, Lyon III, 2011.

PETIT (J.), *Les collectivités locales. Mélanges en l'honneur de Jacques Moreau*, Paris, Economica, 2003, 491 p.

PETITTI (L.-E.), IMBERT (P.-H.) et DECAUX (E.) (dir.), *La Convention européenne des droits de l'Homme. Commentaire article par article*, Paris, Economica, 1995, 1230 p.

PFLIMLIN (E.), *Drones et robots. La guerre des futurs*, Levallois-Perret, Studyrama, 2017.

PHILIPPE (X.), *Le contrôle de proportionnalité dans les jurisprudences constitutionnelle et administrative*, éditions Economica, PUAM, coll. Sciences et droit administratif, Thèse, 1990, 499 p.

PICARD (E.), *La notion de police administrative*, Tome II, Paris, LGDJ, coll. Bibliothèque de droit public, 1984, 926 p.

PIETTE-COUDOL (T.), *Les objets connectés : Sécurité juridique et technique*, Paris, Édition LexisNexis, 2015, 126 p.

POLIN (R.) (dir.), *L'ordre public*, Paris, PUF, 1996, 128 p.

POTASZKIN (T.), *L'éclatement de la procédure pénale : vers un nouvel ordre procédural pénal ?*, Paris, LGDJ, Thèse, 2014, 579 p.

PRÉTOT (X.) et ZACHARIE (C.), *La police administrative*, Paris, LGDJ, coll. Systèmes, 2018, 162 p.

QUÉMÉNER (M.), *Cybercriminalité : droit pénal appliqué*, Paris, éditions *Economica*, 2010, 273 p.

RAZAC (O.), *Après Foucault, avec Foucault : Disséquer la société de contrôle*, Paris, L'Harmattan, 2008.

REDOR (M-J.) (dir.), *L'ordre public : ordre public ou ordres publics ? Ordre public et droits fondamentaux*, Bruxelles, Bruylant, coll. Droit et justice, 2001, 436 p.

RENOUX (T.), *Le Conseil constitutionnel et l'autorité judiciaire. L'élaboration d'un droit constitutionnel juridictionnel*, Paris, Économica, coll. Droit public fondamental, Thèse, 1984, 608 p.

REVET (T.) (dir.), *L'ordre public à la fin du XXème siècle*, Paris, Dalloz, 1996, 111 p.

ROBERT (J.), *Liberté publiques*, Paris, Montchrestien, coll. Université nouvelle, Précis Domat, 1971, 651 p.

ROBERT (X.), *Mélanges Jacques Robert. Libertés*, Paris, Montchrestien, 1998, 608 p.

RODRIGUEZ (E.), *Drones - Missions de secours de sécurité civile*, Paris, Éditions Carlo Zaglia, coll. Les cahiers du savoir, 2019, 82 p.

SADIN (É.), *La vie algorithmique - Critique de la raison numérique*, Paris, Édition L'échappée, coll. « Pour en finir avec », 2015, 288 p.

SAUVAJOL-RIALLAND (C.), *Infobésité : Comprendre et maîtriser la déferlante d'informations*, Paris, Vuibert, 2013, 208 p.

SÈVE (R.), *L'ordre public*, Paris, Dalloz, coll. Archives de philosophie du droit, Tome 58, 2015, 474 p.

SMYTH (S.), *Drone controversies : ethical and legal debates surrounding targeted strikes and electronic surveillance*, Toronto, Thomson Reuters, 2016, 146 p.

SONTAG KOENIG (S.), *Technologie de l'information et de la communication et défense pénale*, Paris, Mare & Martin, Thèse, 2015, 744 p.

SUDRE (F.) (dir.), *Le principe de subsidiarité au sens du droit de la Convention européenne des droits de l'homme*, Bruxelles, Artemis, Némésis, 2014, 412 p.

THÉODOROU (S.) (dir.), *L'État d'exception dans tous ses états*, Marseille, Éditions Parenthèses, 2007, 294 p.

THOMAS-TAILLANDIER (D.), *Contribution à l'étude des procédures dérogatoires*, Aix en Provence, Presses Universitaires d'Aix-Marseille, Thèse, 2014, 423 p.

TOFFLER (A.), *Le choc du Futur*, éd. Denoël, 1971, 539 p.

TOUILLIER (M.) (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Paris, Dalloz, coll. « Les Sens du droit », 2017, 260 p.

TÜRK (A.), *La vie privée en péril, des citoyens sous surveillance*, Paris, Odile Jacob, 2011, 270 p.

VACHER (P.), *Réglementation du pilotage de drones*, Toulouse, Éditions Cépaduès, 2016, 45 p.

VALLAR (C.) et LATOUR (X.) (dir.), *Le droit de la sécurité et de la défense en 2013*, Aix-Marseille, PUAM, 2014, 334 p.

VAUTROT-SCHWARZ (C.) (dir.), *La police administrative*, Paris, PUF, 2014, 320 p.

VAZ-FERNANDEZ (C-A.), *Big Data et Intelligence artificielle de la sécurité intérieure en France*, Paris, L'Harmattan, 2020, 241 p.

VERGÈS (E.), VIAL (G.) et LECLERC (O.), *Droit de la preuve*, Paris, PUF, 2ème édition, 2022, 828 p.

WARUSFEL (B.) et BAUDE (F.), *Annuaire 2018 du Droit de la Sécurité et de la Défense*, Lyon, Mare & Martin, Volume 3, 2018, 434 p.

WEBER (M.), *Le savant et le politique*, Paris, La Découverte, 2003, 210 p.

ZETTER (K.), *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New-York, Crown Publishing Group, 2014.

ZUBELDIA (O.), *Histoire des drones : de 1914 à nos jours*, Paris Perrin, 2012.

III. Articles de doctrine, contributions, fascicules et formulaires

ANDRIANTSIMBAZOVINA (J.), « La protection des libertés, fondement de la compétence du juge administratif ? », *RGD*, chron. « Doits des libertés », 2019.

ANDRIANTSIMBAZOVINA (J.), « Convention européenne des Droits de l'Homme » *in Annuaire international de justice constitutionnelle : Constitution, Libertés et Numérique* 37-2021, 2022, pp. 271-285.

ALLAIS (M.), « Le comportement de l'homme rationnel devant le risque : critiques des postulats et axiomes de l'école Américaine », *Econometrica* n°4, vol. 21, 1953, pp. 503-546.

ARCHAMBAULT (L.) et ROTILLY (C.), « Vers une nouvelle réglementation européenne des drones », *Dalloz IP/IT* n° 3, 22 mars 2021, p. 163.

AUTIN (J-L.), « Fasc. 75 Les autorités administratives indépendantes », *JCl. Administratif*, 20 juillet 2010, màj le 3 janvier 2022.

BADINTER (R.), « Le droit au respect de la vie privée », *JCP G* 1968, I, 2136.

BAROCAS (S.) and SELBST (A.D.), "Big Data's disparate impact", *California Law Review* n° 3, Vol. 104, June 2016, pp. 671-732 [en ligne].

BASDEVANT (A.), « La sécurité de l'usage des drones civils aériens », *RLDI* n°131, 1er novembre 2016, pp. 37-44.

BEAUSSONIE (G.), « Droit à la sécurité contre droit à la sûreté. La liberté est-elle encore le principe ? », *Colloque sous la direction de GAVEN (J-C.) sur : Les ressorts de l'extraordinaire. Justice et police dans la fabrique de l'exception. Perspectives historiques et contemporaines*, Toulouse, 30 et 31 mars 2017, p. 2.

BEAUSSONIE (G.), « Le crépuscule de la sûreté individuelle », *Rec. Dalloz* n° 31, 21 septembre 2017, p. 1768.

BEAUSSONIE (G.), « Le nouvel antagonisme entre sécurité et sûreté (à propos de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme) », *Revue de jurisprudence commerciale* n° 1, janvier/février 2018.

BÉNÉJAT-GUERLIN (M.), « Le droit pénal de la route face aux nouveaux modes de transports », *AJP* n° 9, 25 septembre 2019, p. 428.

BENESTY (G.), « Le clair-obscur du contrôle de la vidéosurveillance », *AJDA* n° 14, 19 avril 2010, p. 764.

BERTAIL (P.), BOUNIE (D.), CLÉMENÇON (S.) et WAELBROECK (P.), « Algorithmes : Biais, Discrimination et Équité », Fondation Abeona et Paris Télécom, février 2019.

BESSE (P.), CASTETS-RENARD (C.) et GARIVIER (A.), « Loyauté des décisions algorithmiques », Contribution au débat public initié par la CNIL : Éthique et Numérique, 2 juin 2017 [en ligne].

BOINE (C.), « Les systèmes d'intelligence artificielle à finalité générale et la proposition de règlement de la Commission européenne », *Dalloz IPT/IT* n° 2, 19 février 2022, p. 79.

BONFORT (A.), COLIN (C.), DEBAETS (E.), SCHMITZ (J.), MARGUIN (J.), VIGNÉ (V.), PALMA-AMALRIC (V.) et MESTARI (Z.), « Autorités administratives indépendantes et libertés – actualités de l'année 2022 », *RDLF*, 27 mars 2023, chron. n° 20.

BOUCHET (M.), « L'utilisation du contrôle de proportionnalité par la Cour de cassation en droit pénal de fond », *RSC* n° 3, 10 novembre 2017, p. 495.

BOUCHET (M.), « Décollage pour l'utilisation des drones par les policiers et gendarmes », *Gaz. Pal.* n°40, 16 novembre 2021, p. 12.

BOUCHET (M.), « Les drones face aux enjeux de droit pénal et de libertés fondamentales », *Dalloz IP/IT* n°6, 20 juin 2022, p. 299.

BOURGEOIS (M.) et TOUZANNE (B.), « Les aéronefs civils télépilotés avec capteurs : des 'drones de droit' », *Communication - Commerce électronique* n°12, décembre 2015, étude 22.

BOUSTA (R.), « La "spécificité" du contrôle constitutionnel français de proportionnalité », *Revue internationale de droit comparé* n°4, Vol. 59, 2007. pp. 859-877.

BUISSON (J.), *in Rép. Pén. Dalloz*, V° « Preuve », 2020.

BUISSON (J.), « Constat d'infractions par caméras et drones dans la prévention des atteintes à l'ordre public », *Procédures* n°6, juin 2022, pp. 11-15.

CAHN (O.), « Un État de (la) police », *RSC* n°4, octobre-décembre 2019, pp. 975-996.

CANIVET (G.), « Positions et composition dans la genèse d'une liberté fondamentale - Les contours de la liberté individuelle dans la jurisprudence du Conseil constitutionnel », Titre VII, *La liberté individuelle* n° 7, octobre 2021.

CAPRIOLI (É.), « Vers un marché unique des acteurs de la cybersécurité », *Communication Commerce électronique* n° 5, mai 2019.

CASTETS-RENARD (C.), « L'IA en pratique : la police prédictive aux États-Unis », *Dalloz IP/IT*, n°5, 15 mai 2019, p. 314.

CASTET-RENARD (C.), « Quel droit de l'intelligence artificielle dans l'Union européenne ? Ou les multiples ambitions normatives de l'*AI Act* », *Dalloz IP/IT* n° 2, 19 février 2022, p. 67.

CAUSSE (H.), « Le principe de sûreté et le droit à la sécurité », *Gaz. Pal.* n°354, 20 décembre 2001, pp. 2-6.

CEYHAN (A.) (dir.), Étude « Gendarmerie et technologie : l'impact de la haute technologie sur la sécurité. Analyse comparée », *Centre de prospective de la gendarmerie Nationale*, 2005.

CHANDER (A.), "The Racist Algorithm?", *Michigan Law Review*, Vol. 115, 2017, pp. 1023-1045.

CHARLES (J-B.) et PARIER (S.), « Les drones dans le viseur des cybercriminels : que dit le droit ? », *Air & Cosmos* n° 2555, 7 juillet 2017, p. 25.

CHARLES (J-B.) et DUPONT (P.), « Fasc. 962 Drones civils - Notion, cadre et régime », *JCl. Transport*, 2 octobre 2018, màj le 31 mars 2021.

CHEVALLIER (J.), « La police est-elle encore une activité régalienne ? », *Archives de politique criminelle* n° 33, vol. 1, 2011, pp. 13 à 27.

CIROTTEAU (M.), « La réception du droit de l'Union par le juge administratif en matière de conservation des données de connexion et de surveillance : la lettre plutôt que l'esprit », *JCP A* n° 50, 19 décembre 2022, étude 2345.

CLARKE (R.), "The regulation of civilian drones' impacts on behavioural privacy", *Computer Law & Security Review Elsevier Ltd*, n°30, 2014, pp. 286-305.

CLAUSEN (F.), « Le contrôle de proportionnalité par la Cour de justice de l'Union européenne », *AJDA* n° 14, 19 avril 2021, p. 800.

COLLET (P.), « La validité contestable de la vidéosurveillance de la voie publique en enquête préliminaire », *JCP G* n° 26, 28 juin 2021, act. 711.

COLLET (P.), « La vidéoprotection et la captation d'images dans la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés », *Communication - Commerce électronique* n°9, septembre 2021, p. 14.

COLLET (P.), « Le recours aux drones validé pour la criminalité organisée ! », *JCP G* n° 1, 9 janvier 2023, act. 18.

COMMARET (D.), « Les métamorphoses de la preuve pénale », *Revue pénitentiaire* n° 4, 2003, pp. 735-744.

COURRÈGES (A.), « Le Conseil constitutionnel apporte des précisions inédites à l'occasion de l'examen de la loi relative aux jeux Olympiques et Paralympiques de 2024 », *DA* n° 7, 1er juillet 2023, 80.

COURTOIS (G.) et GOSSE (N.), « Enjeux juridiques et éthiques des algorithmes », *Revue de la gendarmerie national « Algorithmes et espace normatif »*, 2nd Trimestre 2018, p. 86.

CRICHTON (C.), « Prudence du Parlement européen sur l'utilisation de l'IA par les autorités policières et judiciaires », *Dalloz IP/IT* n° 11, 24 novembre 2021, p. 538.

CROUZATIER-DURAND (F.), « De la vidéosurveillance à la vidéoprotection, une nouvelle conciliation des exigences de sécurité et de liberté ? : À propos de la circulaire du 28 mars 2011 d'application de la Loppsi 2 relative à la prévention de la délinquance », *JCP A* n°22, 30 mai 2011, 2196.

CUSSON (M.), « La surveillance et la télésurveillance : sont-elles efficaces ? », *Revue internationale de criminologie de police technique et scientifique* n° 2, 2005, p. 132.

DANAHER (J.), "The threat of Algocraty : Reality, Resistance and Accommodation", *Philosophy & Technology*, vol. 29 (3), 2016, pp. 245-268.

DANIS-FATÔME (A.), « Sécurité nationale et protection des données : quelle articulation ? », *Communication et commerce électronique* n° 9, septembre 2021, comm. 66.

DANJAUME (G.), « Le principe de la liberté de la preuve en procédure pénale », *Rec. Dalloz* n° 18, 2 mai 1996, p.153.

DARSONVILLE (A.), « Décision n° 2011-625 DC du 10 mars 2011 : une censure sévère de la LOPPSI 2 ? », *Constitutions : Revue de droit constitutionnel appliqué* n°2, 2011, p. 223.

DESGENS-PASANAU (G.), « Traçage des données mobiles : ne sacrifions pas la protection de nos données sur l'autel de la crise sanitaire », *JCP G* n°18, 4 mai 2020, 543.

DELCHER (É.), « La surveillance de masse aux prises avec les droits fondamentaux - dialogue de sourds ou concurrence des juges ? », *RDP* n° 3, 1er mai 2022, p. 845.

DELMAS-MARTY (M.), « Libertés et sûreté : les mutations de l'État de droit », issu du cours « Libertés et sûreté dans un monde dangereux », *Revue de synthèse* n° 3, tome 130, 6ème série, 2009, pp. 465-491 [en ligne].

DELMAS-MARTY (M.), « Sécurité et dangerosité », *RFDA* n°6, 10 janvier 2012, p.1096.

DELVOLVÉ (P.), « Les contradictions de la délégation de service public », *AJDA*, 1996, p. 677.

DELVOLVÉ (P.), « Sécurité et sûreté », *RFDA* n°6, 10 janvier 2012, p. 1085.

DE MONTALIVET (P.), « Les objectifs de valeur constitutionnelle », *Cahiers du Conseil constitutionnel* n° 20, juin 2006.

DE MONTECLER (M-C.), « Ô drone, reprends ton vol ! », *AJDA* n° 16, 1er mai 2023, p. 813.

DOEBELIN (V.), « Allô les secours... ? Allô ? ! », *JCP A* n° 35, 30 août 2021, act. 502.

DROIN (A.), DUBOYS FRESNEY (M.), MAULIN (C.) et VINCENT (A.), « Actualité Informatique et Libertés - Déploiements de caméras "augmentées" : sous quelles conditions ? », *AJDA* n° 39, 21 novembre 2022, p. 2223.

DUPRÉ DE BOULOIS (X.), « Existe-t-il un droit fondamental à la sécurité ? », *RDLF*, 2018, chron. 13.

DUPRÉ DE BOULOIS (X.), « Des droits de l'homme au service de la puissance de l'État », *RDLF*, 2022, chron. 2.

DUCLERQ (J-B.), « Sécurité des systèmes d'information de l'Administration : quelles garanties pour les administrés ? », *RDP* n° 5, 1er septembre 2020, p. 1213.

EDDAZI (F.), « L'association du secteur privé à l'exploitation des données policières », *RDP* n°1, 1er janvier 2018, p. 189.

FERAL-SCHUHL (C.), « La collecte de la preuve numérique en matière pénale », *AJP* n° 3, 2009, p. 115.

FEUTEUN (C.) et RIMSEVICA (D.), « Cloud Act et cloud computing : une menace pour les données ? », *Revue de Droit bancaire et financier* n° 5, septembre 2020, dossier 27.

FINN (R.) *et al.*, "Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations", *Publications Office of the European Union*, 2014. 38 p.

FRAISSE (R.), « Le Conseil constitutionnel exerce un contrôle conditionné, diversifié et modulé de la proportionnalité », *LPA* n° 46, 5 mars 2009, p. 74.

FROMENT (J-C.), « Regard juridique sur la vidéosurveillance urbaine : un droit en trompe-l'œil », *JCP A* n° 13, 27 mars 2006, pp. 435-440.

FROMONT (M.), « Le principe de proportionnalité », *AJDA* n° HS, 20 juin 1995, p. 156.

GAUTHIER (C.), « Le contrôle de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme », *AJDA* n° 14, 19 avril 2021, p. 793.

GILL (M.) and FISCHER (P.), "Does CCTV displace crime ?", *Criminology and Criminal Justice* n°2, vol. 9, 2009, pp. 207-224.

GLEIZAL (J-J.), « La sécurité : une nouvelle politique », *RFAP* n° 91, 1999, p. 369.

GOHIN (O.), « La Constitution, ultime obstacle à la privatisation de la sécurité ? », *Les Cahiers de la sécurité* n° 19, mars 2012, pp. 18-26.

GOJKOVIC-LETTE (J.) et HOUILLON (G.), « La pratique du drone, entre sécurisation et répression », *AJP* n°3, 26 mars 2019 p. 135.

GOSEL-LE BIHAN (V.), « Le contrôle de proportionnalité au Conseil constitutionnel », *AJDA* n° 14, 19 avril 2021, p. 786.

GRANGER (M-A), « Existe-t-il un « droit fondamental à la sécurité » ? », *RSC* n°2, 15 juin 2009, pp. 273-296.

GUÉRIN (D.), « La loyauté de la preuve devant le juge pénal », *Procédures* n° 4, 2015, Dossier 11.

GUINIER (D.), « Sécurité : Vulnérabilité aux cyberattaques du GPS à usage civil », *Expertises des systèmes d'information* n°3, mars 2017, pp.108-112.

HANICOTTE (R.), « Espace public, impasse des libertés », *JCP A* n° 26, 2 juillet 2012, 2227.

HANICOTTE (R.), « Une nouvelle catégorie d'OVNI juridique: les drones », *Gaz. Pal.* n°317, 13 novembre 2014, p. 6.

HAYEZ (P.), « La Cour des comptes : du contrôle à l'évaluation », *Revue française d'Administration publique* n°3, 2015, pp. 707-711.

HEILMANN (É.), « La vidéosurveillance, une réponse efficace à la criminalité ? », *Criminologie*, vol. 1, 2003, pp. 89-102.

HERRAN (T.), « L'impact de la loi relative à la sécurité publique sur la distinction entre la police judiciaire et la police administrative », *AJ Pénal* n° 11,16 novembre 2017, p. 472.

HOCHMANN (T.), « Un succès d'exportation : la conception allemande du contrôle de proportionnalité », *AJDA* n° 14, 19 avril 2021, p. 805.

HO-DAC (M.), « La normalisation, clé de voûte de la règlementation européenne de l'intelligence artificielle (*AI Act*) », *Dalloz IP/IT* n° 4, 20 avril 2023, p. 228.

JOBART (F.) et LEVY (R.), Étude « Police et minorités visibles : les contrôles d'identité à Paris », *Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales (CESDIP)*, juillet 2009.

KEATS CITRON (D.) and PASQUALE (F.), "The Scored Society: Due Process for Automated Predictions", *Washington Law Review*, Vol. 89, April 23rd 2014.

KOERING-JOULIN (R.), « Fasc. 620 - Droit à la sûreté », *JCl. Libertés*, 20 septembre 2007.

LAGASSE (J.), « Algorithmes et politiques publiques de sécurité, quels nouveaux paradigmes ? », *Revue de la Gendarmerie nationale*, 2nd Semestre 2018, pp. 47- 54.

LASSALLE (M.), « À la recherche du principe de légalité procédurale en matière pénale », *Rec. Dalloz*, 2020, p. 1196.

LATOUR (X.), « La place du secteur privé dans la politique moderne de sécurité », *AJDA*, 2010, p. 657.

LATOUR (X.) et MOREAU (P.), « Le Conseil national des activités privées de sécurité et la moralisation de la sécurité privée », *JCP A* n° 15, 11 avril 2011, 2146.

LATOUR (X.), « Sécurité publique et sécurité privée, de l'ignorance à la coproduction », *Cahiers de la sécurité* n° 19, 2012, p. 11.

LATOUR (X.) et MOREAU (P.), « Délégation et activités de police : stop ou encore ? », *JCP A* n° 15, 15 avril 2012, 2117.

LATOUR (X.), « Sécurité intérieure : un droit "augmenté" », *AJDA* n° 8, 5 mars 2018, p. 431.

LAZARO (C.), « Le pouvoir "divinatoire" des algorithmes : de la prédiction à la préemption du futur », *Anthropologie et Sociétés*, Vol. 42, n°2-3, 2018, pp. 127-150.

LAZERGES (C.) et ROUSSEAU (D.), Commentaire sous décision C. const., Décision n° 2003-467 DC, 13 mars 2003, 2003.

LAZERGES (C.), « Le choix de la fuite en avant au nom de la dangerosité », *RSC*, janvier/mars 2012, pp. 274-283.

LAZERGES (C.), « Les droits de l'homme à l'épreuve du terrorisme », *RSC* n° 3, 23 novembre 2018, p. 753.

LAZERGES (C.), « Le droit à la sécurité a-t-il effacé le droit à la sûreté ? L'exemple de la loi « Sécurité globale » », *La Revue des droits de l'homme* n° 20, 2021, mis en ligne le 22 juin 2021.

LAZERGES (C.), « La dangerosité de la notion de dangerosité en droit pénal », *Criminocorpus* n° 20, 2022.

LE BONNIEC (N.), « La Cour européenne des droits de l'homme face aux nouvelles technologies de l'information et de communication numériques », *RDLF* 2018, chron. n° 5.

LECLERC (H.), « De la sûreté personnelle au droit à la sécurité », *JDJ - RAJS* n°255, mai 2006, pp. 7-10.

LE GOFF (T.), « La vidéosurveillance est-elle une réponse efficace à la délinquance ? », *AJP* n° 6, 11 juin 2010, p. 275.

LE GOFF (T.) et FONTENEAU (M.), « Vidéosurveillance et espaces publics, État des lieux des évaluations menées en France et à l'étranger », IAU-RIF, Paris, 1er octobre 2008.

LE GOFF (T.) et HEILMANN (É.), « Vidéosurveillance : un rapport qui ne prouve rien », *Délinquance, justice et société*, 24 septembre 2009.

LELIEUR (J.), « L'intelligence artificielle : une nouvelle technologie probatoire en émergence », *AJP* n° 3, 30 mars 2023, p. 112.

LEMAIRE (E.), « Actualité du principe de prohibition de la privatisation de la police », *AJDA*, 2009, p. 767.

LEQUESNE ROTH (C.), « Interview de Caroline Lequesne sur la reconnaissance faciale dans l'espace public : bilan et perspectives européennes », *Dalloz IP/IT* n°6, 20 juin 2020, p. 332.

LOHRER (D.), « Le défenseur des droits : quel bilan après dix ans d'activité ? », *RFDA*, janvier-février 2021, étude pp. 73-86.

LUCHAIRE (F.), « La sûreté : droit de l'homme ou sabre de M. Prudhomme », *RDP*, 1989, pp. 609 et suiv.

MARTI (G.), CLUZEL-MÉTAYER (L.) et MERABET (S.), « Droit et Intelligence artificielle », *JCP G* n° 26, 28 juin 2021, doctr. 720.

MATHIS (B.), « Proposition de règlement européen sur l'intelligence artificielle : le regard d'un praticien », *RLDI* n° 192, mai 2022, pp. 40-44.

MATTATIA (F.), « Gouvernance de la sécurité numérique des administrations », *JCP A* n° 23, 13 juin 2022, act. 394.

MATTATIA (F.), « Expérimentation de caméras intelligentes pour les JO de 2024 : quel encadrement juridique ? », *JCP A* n° 4, 30 janvier 2023, 2028.

MAZEAUD (P.), « La place des considérations extra-juridiques dans l'exercice du contrôle de constitutionnalité » *in 8ème séminaire des cours constitutionnelles tenu à Erevan du 2 au 5 octobre 2003, Les principaux critères de limitation des droits de l'Homme dans la pratique de la justice constitutionnelle*, p. 4.

MAZEAUD (V.), « La constitutionnalisation du droit au respect de la vie privée », *Les nouveaux cahiers du Conseil constitutionnel* n° 48, juin 2015.

MEILLER (Y.), « Intelligence artificielle, sécurité et sûreté », *Sécurité et stratégie* n° 28, janvier 2018, pp. 75-84.

MESA (R.), « Intelligence artificielle et droit pénal : quels responsables, quelles infractions, quelles responsabilités ? », *RLDI* n° 181, mai 2021, pp. 34-39.

MORALES (M.), « L'interdiction de déléguer à une personne privée une compétence de police administrative : une règle inhérente à l'identité constitutionnelle de la France », *DA* n°2, février 2022, comm. 10.

MOREAU (J.), « De l'interdiction faite à l'autorité de police d'utiliser une technique d'ordre contractuel », *AJDA*, 1965, p. 3.

MOREL (B.), « L'attribution d'activités de police à des personnes privées », *RDP*, 1er janvier 2020, p. 77.

MOREL (J-F.) et ABELLARD (M.), « L'emploi des drones, de la gendarmerie au maintien de l'ordre », *Revue de la gendarmerie nationale* n° 267, juin 2020, pp. 121-129.

MORIN-MARTEL (A.), "Machine learning in bail decisions and judges' trustworthiness", *AI &* Soc, April 21st 2023 [en ligne].

MUCCHIELLI (L.), « À quoi sert la vidéosurveillance ? », *VST* n°154, février 2022, pp. 23-29.

OBERDORFF (H.), « Le droit, la démocratie et la maitrise sociale des technologies », *RDP*, 1992, p. 983.

OSWALD (M.), GRACE (J.), URWIN (S.) AND BARNES (G.), "Algorithmic risk assessment policing models : lessons from the Durham HART model an 'experimental' proportionality information & communications technology law", *Information & Communications Technology Law*, August 31st 2017.

PAPINEAU (C.), « Enjeux éthiques et juridiques des algorithmes au regard des missions de sécurité publique », *Revue de la Gendarmerie Nationale*, 2nd Semestre 2018, pp. 21-25.

PARROT (K.), « La proposition de loi sur la « sécurité globale » poursuit subrepticement une transformation sécuritaire de la politique pénale », *JCP G* n° 13, 29 mars 2021, 367.

PAUVERT (B.), « L'utilisation des drones à l'appui de la sécurité », *JCP A* n°27, 5 juillet 2021, p. 2220.

PÉGNY (M.) et IBNOUHSEIN (M.I.), « Quelle transparence pour les algorithmes d'apprentissage machine ? », *INRIA*, 14 mai 2018.

PELLÉ (S.), « De la responsabilité pénale, du trouble mental et de quelques dispositions en matière de sécurité intérieure », *Rec. Dalloz*, 2022, p. 519.

PIGNATEL (L.), « Pas de nullité de principe des opérations de captation d'images réalisés par drone », *Dalloz act.* n° 29, 29 novembre 2022.

POIRAT (F.), « La doctrine des « droits fondamentaux » de l'État », *Droits*, 1992, p. 83.

PONS (R.) et RISSER (L.), « Biais et discriminations dans les systèmes d'intelligence artificielle », *Dalloz IP/IT* n°2, 19 février 2022, p. 75.

POURCEL (E.), « Drone aérien : y-a-t-il un pilote « de » l'avion ? », *JCP G* n°49, 30 novembre 2015, 1312.

PRAT (M-P.) et JANVIER (C.), « La Cour des comptes auxiliaire de la démocratie », *Pouvoirs* n° 3, 2010 pp. 97-107.

PRÉTOT (X.), « Le pouvoir de police ne se concède pas : un principe inhérent à l'identité constitutionnelle de la France à la portée toute relative… », *JCP A* n° 48, 6 décembre 2021, 2373.

RENUCCI (J-F.), « Intime conviction, motivation des décisions de justice et droit à un procès équitable », *Recueil Dalloz*, 2009, p. 1058.

RIVERO (J.), « Liberté individuelle et fouille des véhicules », note sous C. const., Décision n° 76-75 DC, 12 janvier 1977, *AJDA* 1978, pp. 215-216.

RIVERO (J.), « Dualité de juridictions et protection des libertés », *RFDA*, 1990, p. 736.

ROCHFELD (J.), « L'encadrement des décisions prises par algorithme », *Dalloz IP/IT* n°9, 12 septembre 2018, p. 474.

ROLIN (F.) et SLAMA (S.), « Les libertés dans l'entonnoir de la législation anti-terroriste : Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers », *AJDA* n°18, 15 mai 2006, p. 975.

ROUSSEAU (D.), « Chronique de jurisprudence constitutionnelle 1993-1994 », *RDP* 1995, pp. 51-104.

ROUSSEAU (D.), « Sécurité globale : une vrai-fausse proposition de loi, une vrai privatisation de la surveillance, des réserves et censures ambigües », *Gaz. Pal.* n°21, 8 juin 2021, p. 19.

ROUSSEL (S.), « Le contrôle de proportionnalité dans la jurisprudence administrative », *AJDA* n° 14, 19 avril 2021, p. 780.

RUEGG (J.) (dir), Rapport « Vidéosurveillance et risques dans l'espace à usage public - Représentations des risques, régulation sociale et liberté de mouvement », CETEL, Université de Genève et de Fribourg, octobre 2006.

SAFI (F.), « La loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement : Entre pérennisation et extension de l'exception… », *JCP G* n° 40, 4 octobre 2021, 1012.

SAINT-PAU (J-C.), « Fasc. 20 : Vidéoprotection », *JCl Lois pénales spéciales*, 21 mars 2016.

SAURON (J-L.), « Les autorités de contrôles de protection des données un point d'étape de leurs moyens et de leur pratique », *RLDI* n° 186, novembre 2021, pp. 36-41.

SAUVAJOL-RIALLAND (C.), « Infobésité, gros risques et vrais remèdes », *L'expansion Management Review* n° 152, 2014, pp. 110-118.

SAUVÉ (J-M.), « Le juge administratif et les droits fondamentaux », *AJDA* n° 43, 19 décembre 2016, p. 2420.

SAUVÉ (J.-M.), « Le principe de proportionnalité, protecteur des libertés ? », *Les cahiers de Portalis* n° 5, 2018, pp. 11 et suiv.

SCHRAMECK (O.), « Sécurité et libertés », *RFDA*, 2011, p. 1093.

SIBER (J.), « L'image et le manifestant », *Gaz. Pal.* n°4, 24 janvier 2017, p. 81.

SIMON (D.), « Le contrôle de proportionnalité exercé par la Cour de justice des Communautés européennes », *LPA*, 5 mars 2009, n° 46, p. 17.

SIZAIRE (V.), « Le juge administratif et la protection des libertés. Éléments pour une garde partagée », *RDLF*, 2019, chron. n° 27.

SONTAG-KOENIG (S.), « Sonorisation et fixation d'images : que reste-t-il de la vie privée ? », *AJP* n° 1, 30 janvier 2023, p. 27.

STABEN (J.), « Der Abschreckungseffekt auf die Grundrechtsausübung : Strukturen eines verfassungsrechtlichen Arguments », *Mohr Siebeck*, 2016.

SUDRE (F.), « La mise en quarantaine de la Convention européenne des droits de l'homme », *JCP G* n° 17, 27 avril 2020, act. 510.

SUDRE (F.), « Droit au respect de la vie privée - Protection des données personnelles dans le cadre d'une procédure pénale », *JCP-G* n° 26, 3 juillet 2023, act. 810.

TOUATI (A.), NINO (G.), ELKOUBI (A.) et KOUM DISSAKE (V.), « La reconnaissance faciale, entre sécurité et droits fondamentaux », *Revue pratique de la prospective et de l'innovation* n° 2, 1er octobre 2019, p. 2.

TOUZÉ (S.), « La restriction vaudra toujours mieux que la dérogation… », *JCP G* n° 17, 27 avril 2020, act. 511.

VIANGELLI (F.), « Des données à la responsabilité : de l'anonymisation à l'attaque par réidentification », *RLDI* n° 173, août-septembre 2020, pp. 40-45.

VIGNEAU (V.), « Libres propos d'un juge sur le contrôle de proportionnalité », *Recueil Dalloz*, 2017, p. 123.

VITALIS (A.), « Vidéosurveillance et libertés individuelles », *Revue de la gendarmerie nationale* n° 199, 2ème trimestre 2001, p. 25.

WARUSFEL (B.), « Les notions de défense et de sécurité en droit français », *Droit & Défense* 94/4, octobre 1994, p. 11.

WARUSFEL (B.), « Enjeux et limites de l'ouverture des données en matière de sécurité et de défense », *Revue française d'administration publique* n° 167, mars 2018.

WARUSFEL (B.), « La place de l'image : caméras et vidéoprotection dans la sécurité globale », *JCP A* n°27, 5 juillet 2021, 2219.

WARUSFEL (B.), « La LOPMI et la transformation numérique des moyens de la sécurité intérieure », *JCP A* n° 13, 3 avril 2023, 2099.

WATIN-AUGOUARD (M.), « La cybersécurité, enjeu de la souveraineté à l'ère numérique », *Dalloz IP/IT* n° 3, 22 mars 2021, p. 130.

YOUHNOVSKI SAGON (A-L.), « Les recommandations du Défenseur des droits : un couteau suisse au service du respect des droits et libertés fondamentaux », *Droit administratif* n° 11, novembre 2022, étude 12.

ZILLER (J.), « Le principe de proportionnalité », *AJDA* n° HS, 10 juin 1996, p. 85.

ZLIOBAITE (I.) and CUSTERS (B.), "Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models", *Artificial Intelligence and Law* (24), October 7th 2016, pp. 183-201.

IV. Contributions en sciences informatiques et médicales (illustrations)

AELES (J.) *et al.*, "Revealing the unique features of each individual's muscle activation signatures", *J R Soc Interface*, January 18th 2021.

BANSAL (A.), MA (S.), RAMANAN (D.) and SHEIKH (Y.), "Recycle-GAN: Unsupervised Video Retargeting", *European Conference on Computer Vision* (ECCV), 2018.

BARADEL (F.), WOLF (C.), MILLE (J.) and TAYLOR (G. W.), "Glimpse Clouds: Human Activity Recognition from Unstructured Feature Points", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2018, pp. 469-478 [en ligne].

BARREDO ARRIETA (A.) and *al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI", *Information Fusion*, Vol. 58, June 2020, pp. 82-115.

BERK (R.) *et al.*, "Fairness in criminal justice risk assessments : The state of the art", June 26th 2018.

BERMEJO (E.), DENIZ (O.), BUENO (G.) and SUKTHANKAR (R.), "Violence Detection in Video Using Computer Vision Techniques", *International Conference on Computer Analysis of Images and Patterns* (CAIP) 2011, pp. 332-339 [en ligne].

BESSE (P.) *et al.*, "A Survey of Bias in Machine Learning Through the Prism of Statistical Parity", *The American Statistician*, July 2nd 2021, pp. 188-198.

BIAU (D-J.), JOLLES (B.M.) and PORCHER (R.), "P Value and the Theory of Hypothesis Testing: An Explanation for New Researchers", *Clin Orthop Relat Res* 468(3), 2010, pp. 885–892.

BIGGIO (B.) and ROLI (F.), "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning", *Pattern Recognition*, Vol. 84, December 2018, pp. 317-331.

BLOCK (C. J.), KOCH (S.M.), LIBERMAN (B.E.), MERRIWEATHER (T.J.) and ROBERSON (L.) "Contending With Stereotype Threat at Work: A Model of Long-Term Responses", *The Counseling Psychologist* n°39, Vol.4, 2011, pp. 570-600.

BOLOGNA (G.) and HAYASHI (Y.), "Characterization of symbolic rules embedded in deep dimlp networks: A challenge to transparency of deep learning", *Journal of Artificial Intelligence and Soft Computing Research* n°4, Vol. 7, 2017, pp. 265-286.

BOLUKBASI (T.), CHANG (K-W.), ZOU (J.), SALIGRAMA (V.) and KALAI (A.), "Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings", 30th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain, 2016.

BROWN (T.) *and al.*, "Adversarial Patch", *31st Conference on Neural Information Processing Systems* (NIPS 2017), May 17th 2018.

BUOLAMWINI (J.) and GEBRU (T.), "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *PMLR* 81, 2018, pp. 1-15.

BURRELL (J.), "How the machine "thinks" : Understanding opacity n machine learning algorithms", *Big Data Society*, 2016 p. 4.

CHEN (D.) *et al.*, "Recognition of Aggressive Human Behavior Using Binary Local Motion Descriptors", *Annual International Conference IEEE Eng Med Biol Soc.* 2008 [en ligne].

CHEONG (K.H.) *et al.*, "Practical Automated Video Analytics for Crowd Monitoring and Counting", *IEEE*, vol. 7, January 2019 [en ligne].

CORBETT-DAVIES (S.) *et al.*, "The Measure and Mismeasure of Fairness: A Critical Review of Fair Machine Learning", *Journal of Machine Learning Research* 24, 2018 (revised in August 2023).

CUMMINGS (M. L.), "Automation and accountability in decision support system interface design", *Journal of Technology Studies* n° 1, vol. 32, 2006.

DE-ARTEAGA (M.) *et al.*, "Bias in Bios: A Case Study of Semantic Representation Bias in a High-Stakes Setting", *ACM Conference on Fairness, Accountability, and Transparency*, January 27th 2019.

DEMPSEY (R.P.), BRUNET (J.R.) and DUBLJEVIĆ (V.), "Exploring and Understanding Law Enforcement's Relationship with Technology: A Qualitative Interview Study of Police Officers in North Carolina", *Applied Sciences*, March 18th 2023.

DE SMEDT (Q.), WANNOUS (H.), VANDEBORRE (J-P.), "Skeleton-based Dynamic hand gesture recognition", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2016, pp. 1206-1214 [en ligne].

EASTON (R.) and FRAZIER (E.), "GPS Declassified : From Smart Bombs to Smartphones", *Technology and Culture* 57 (1), January 2016, pp. 276-278.

ELSAYED (G.F.), GOODFELLOW (I.) and SOHL-DICKSTEIN (J.), "Adversarial Reprogramming of Neuronal Network", November 29th 2018.

EYKHOLT (K.) *and al.*, "Robust Physical-World Attacks on Deep Learning Visual Classification", *CVPR 2018*, April 10th 2018.

FAN (J.), FANG (H.) and HAN (L.), "Challenges of Big Data Analysis", *National Science Review* 1(2), October 26, 2013, pp. 293-314.

FARRINGTON (D.), GILL (M.), WAPLES (S.) and ARGOMANIZ (G.), "The effects of closed-circuit television on crime: meta-analysis of an English national quasi-experimental multi-site evaluation", *Journal of Experimental Criminology* n° 3, 2007, pp. 21-38.

FELDMAN BARRETT (L.), *How Emotions Are Made: the Secret Life of the Brain*, New York, Houghton Mifflin Harcourt. [2017] ; LERNER (J.S.), LI (Y.), VALDESOLO (P.) and KASSAM (K.S.), "Emotion and decision-making", *Annual Review of Psychology*, 66, 2015, pp. 799-823.

FREDERICK (S.), "Cognitive reflection and decision making", *Journal of Economic Perspectives* n°4, vol. 19, 2005, pp. 25-42.

FREDRIKSON (M.), JHA (S.) and RISTENPART (T.), "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures", *ACM CCS'15,* October 12–16, 2015.

FRIEDLER (S.) *et al.*, "On the (im)possibility of fairness", 2016.

GOHEL (P.), SINGH (P.) and MOHANTY (M.), "Explainable AI: current status and future directions", *Computer Science*, July 12th 2021.

GOODFELLOW (I.) *and al.*, "Generative Adversarial Nets", *NIPS'14: Proceedings of the 27th International Conference on Neural Information Processing Systems*, Vol. 2, December 2014, pp. 2672–2680.

GOODFELLOW (I.), SHLENS (J.) and SZEGEDY (C.), "Explaining and harnessing adversarial examples", *ICLR*, 2015.

GRGIĆ-HLAČA (N.), REDMILES (E. M.) GUMMADI (K. P.) and WELLER (A.), "Human Perceptions of Fairness in Algorithmic Decision Making: A Case Study of Criminal Risk Prediction", *in WWW 2018: The 2018 Web Conference*, April 23–27 2018, 10 p. [en ligne].

GUNNING (D.) and *al.*, "Explainable Artificial Intelligence (XAI)", *Science Robotics*, Vol. 4 (37), December 18th 2019.

HASSNER (T.), ITCHER (Y.) and KLIPPER-GROSS (O.), "Violent Flows: Real-Time Detection of Violent Crowd Behavior", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2012, pp. 1-6 [en ligne].

HAYDA (M.) and RAKOVA (B.), "Enhanced well-being assessment as basis for the practical implementation of ethical and rights-based normative principles for AI". *2020 IEEE International Conference on Systems, Man, and Cybernetics*, 2020, pp. 2754-2761 [en ligne].

HAYES (J.) et al., "LOGAN: Membership Inference Attacks Against Generative Models", *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2019, Issue 1. August 21st 2018.

HE (K.), ZHNG (X.), REN (S.) and SUN (S.), "Deep Residual Learning for Image Recognition", *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770-778 [en ligne].

HONG (S.) *and al.*, "A Panda ? No, It's a Sloth : Slowdown Attacks on Adaptative Multi-Exit Neural Network Inference", *ICLR 2021*, February 25th 2021.

HORST (F.) *et al.*, "Explaining the unique nature of individual gait patterns with deep learning", *Sci Rep.*, February 20th 2019, 2391.

HUG (F.) *et al.*, "Individuals have unique muscle activation signatures as revealed during gait and pedaling", *J Appl Physiol* (1985), October 1st 2019, 127(4), pp.1165-1174.

JI (N.) *and al.*, "Adversarial YOLO: Defense Human Detection Patch Attacks via Detecting Adversarial Patches", March 16*th* 2021.

KAHNEMAN (D.), SLOVIC (P.) and TVERSKY (A.), "Judgment under Uncertainty: Heuristics and Biases", *Science*, New Series n° 185, 1974, pp. 1124-1131.

KE (S.) *et al.*, "A Review on Video-Based Human Activity Recognition", *Computers*, vol. 2, June 5th 2013, pp. 88–131 [en ligne].

KHAKUREL (U.) and RAWAT (D.B.), "Evaluating Explainable Artificial Intelligence: Algorithmic Explanations for Transparency and Trustworthiness", *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications IV*, Vol. 12113, June 6th 2022.

KITANI (K.M.), ZIEBART (B.D.), BAGNELL (J.A.) and HEBERT (M.), "Activity Forecasting", *Computer Vision – ECCV* 2012 [en ligne].

KLEINBERG (J.) and *al.*, "Human Decisions and Machine Predictions", *The Quarterly Journal of Economics*, Oxford University Press, vol. 133(1), 2018, pp. 237-293.

KNIGHT (W.). "The Dark Secret at the Heart of IA", *The MIT Technological Review*, 120 (3), 2017.

LOFTUS (J. R.) *et al.*, "Causal Reasoning for Algorithmic Fairness", June 6th 2018.

NELSON (B.) *et al.*, "Exploiting Machine Learning to Subvert Your Spam Filter", *1st USENIX Workshop on Large Scale Exploits and Emergent Threats*, April 2008.

NGAN (M.) and GROTHER (P.), "Tattoo recognition technology - challenge (Tatt-C): an open tattoo database for developing tattoo recognition research", *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)*, 2015, pp. 1-6 [en ligne].

PEDRESHI (D.) *et al.*, "Discrimination-aware Data Mining", International Conference on *Knowledge Discovery and Data Mining*, 2008, pp. 560-568.

PIZA (E), WELSH (B.), FARRINGTON (D.) and THOMAS (A.), "CCTV surveillance for crime prevention : A 40-year systematic review with meta-analysis", *Criminology & Public Policy* 18(1), March 24th 2019, pp. 135-159.

RIGAKI (M.) and GARCIA (S.), "A Survey of Privacy Attacks in Machine Learning", April 1st 2021.

RYOO (M. S.), "Human Activity Prediction : Early Recognition of Ongoing Activities from Streaming Videos", *2011 International Conference on Computer Vision*, Barcelona, Spain, 2011, pp. 1036-1043 [en ligne].

SABLAYROLLES (A.) *et al.*, "Radioactive data: tracing through training", February 3rd 2020.

SAMEK (W.) *et al.,* "Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models", August 28th 2017.

SANCHEZ-DELACRUZ (E.) *et al.*, "Gait Recognition in the Classification of Neurodegenerative Diseases", *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services. UCAmI 2014*, December 2014, pp. 128-135 [en ligne].

SANDVIG (K.) *et al.*, "Auditing algorithms: Research methods for detecting discrimination on internet platforms", *64th Annual Meeting of the International Communication Association*, May 22nd 2014.

TADDEO (M.) et FLORIDI (L.), "Regulate artificiel intelligence to avert cyber arms race", *Nature*, vol. 29 (3), 2018, pp. 296-298.

VEALE (M.), BINNS (R.), EDWARDS (L.), "Algorithms that remember: model inversion attacks and data protection law", *Phil. Trans. R. Soc. A* 376, July 12th 2018.

WELSH (B.) and FARRINGTON (D.), "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis", *Justice Quarterly* n° 26, October 12th 2009, pp. 716-745.

YIN (M.) *and al.*, "ADC: Adversarial attacks against object Detection that evade Context consistency checks", *2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2022, pp. 2836-2845.

WU (H.) *and al.*, "Adversarial Detection: Attacking Object Detection in Real Time", *IEEE Intelligent Vehicle Symposium, 2023*, May 31st 2023.

ZHANG (Y.) *et al.*, "The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks", April 18th 2020.

ZENGWEI (H.) *et al.*, "Deep Age Distribution Learning for Apparent Age Estimation", *IEEE Conference on Computer Vision and Pattern Recognition* (CVPR), 2016 [en ligne].

V. Documents officiels et rapports

Textes nationaux :

- **Travaux parlementaires**

- **Assemblée nationale**

AN, Compte-rendu intégral, 2ème séance, 11 juin 1980, *JO* Déb. AN 1980, p. 1749.

AN, Séance du 29 mai 2008, *JOAN* du 30 mai 2008, n° 41, p. 2711.

AN, Rapport d'information sur « la contribution de l'État au développement de la vidéoprotection » présenté par GEOFFROY (G.), 13 juillet 2010, 33 p.

AN, Rapport d'information n° 4113 sur « la mise en œuvre des conclusions de la mission d'information sur les fichiers de police » délivré par BATHO (D.) et BÉNESTI (J-A.) le 21 décembre 2011, 229 p.

AN, Rapport n° 2678 sur la proposition de loi relative à la légitime défense des policiers remis par CIOTTI (É.) le 25 mars 2015.

AN, Compte rendu n° 53 (2017-2018) Commission de la défense nationale et des forces armées - Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire.

AN, Rapport n°2111 fait au nom de la Commission d'enquête sur la situation, les missions et les moyens des forces de sécurité, qu'il s'agisse de la police nationale, de la gendarmerie ou de la police municipale, rapporté par AEGELEN (C.), 3 juillet 2019.

AN, Proposition de loi n°3452 relative à la sécurité globale, présenté par FAUVERGUE (J-M.) et THOUROT (A.) le 20 octobre 2020.

AN, Rapport n° 3527 sur la proposition de loi relative à la sécurité globale, 5 novembre 2020.

AN, Débats publics de la troisième séance du vendredi 20 novembre 2020 relatifs à l'amendement n°1164.

AN, Proposition de loi n°599 pour une sécurité globale préservant les libertés, 15 avril 2021.

AN, Projet de loi n°4387 relatif à la responsabilité pénale et à la sécurité intérieure, présenté par DUPONT-MORETTI (É.) et DARMANIN (G.) le 20 juillet 2021.

AN, Texte n°939, adopté par la commission, sur le projet de loi, adopté par le Sénat relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 9 mars 2023.

- **Sénat**

Sénat, Compte rendu intégral des débats du Sénat, 20 janvier 2004.

Sénat, Séance du 24 juin 2008, *JO Sénat* du 25 juin 2008, n° 51, p. 3392.

Sénat, Rapport d'information n°131 (2008-2009) sur « La vidéosurveillance : pour un nouvel encadrement juridique » présenté par COURTOIS (J-P.) et GAUTHIER (C.), 10 décembre 2008.

Sénat, Rapport d'information n° 441 (2008-2009) « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information » remis au nom de la commission des lois par DÉTRAIGNE (Y.) et ESCOFFIER (A-M.), 27 mai 2009.

Sénat, Séance du 27 avril 2016 Débats portant sur le projet de loi pour une République numérique.

Sénat, Rapport d'information n° 464 (2016-2017) « Pour une intelligence artificielle maîtrisée, utile et démystifiée » remis par DE GANAY (C.) et GILLOT (D.), 15 mars 2017.

Sénat, Rapport d'information n° 559 (2016-2017) « Drones d'observation et drones armés : un enjeu de souveraineté », remis par PERRIN (C.) *et al.*, fait au nom de la Commission des affaires étrangères, de la défense et des forces armées, 23 mai 2017.

Sénat, Rapport n°612 fait au nom de la commission d'enquête intitulé « Vaincre le malaise des forces de sécurité intérieure : une exigence républicaine », déposé par GROSDIDIER (F.), 27 juin 2018.

Sénat, Rapport d'information n° 82 sur la sécurité informatique des pouvoirs publics délivré par BASCHER (J.) le 22 octobre 2019.

Sénat, Rapport n°46 (2021-2022) sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, remis par JOURDA (M.) et HERVÉ (L.), 13 octobre 2021.

Sénat, Rapport d'information fait au nom de la commission des lois n° 627 (2021-2022) remis par DAUBRESSE (M-P.), de BELENET (A.) et DURAIN (J.) sur « la reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », 10 mai 2022.

Sénat, Rapport d'information n° 483 (2022-2023) fait au nom de la commission des affaires européennes « relatif à la proposition de législation européenne sur l'intelligence artificielle » remis par GATTOLIN (A.), MORIN-DESAILLY (C.), PELLEVAT (C.) et SCHALCK (E.), 30 mars 2023.

Sénat, Proposition de loi n° 128 relative à la reconnaissance biométrique dans l'espace public, 12 juin 2023.

- **Rapports de mission parlementaire et rapports législatifs**

Rapport de l'office parlementaire d'évaluation de la législation n° 404 (2005-2006) sur « Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié » remis par GÉLARD (P.), 15 juin 2006.

Rapport de la mission Parlementaire, « D'un *continuum* de sécurité vers une sécurité globale » remis par THOUROT (A.) et FAUVERGUE (J-M.), septembre 2018.

Rapport de mission Parlementaire, « Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne » remis par VILLANI (C.), 28 mars 2018, 235 p.

Rapport au Premier ministre, « Pour un usage responsable et acceptable par la société des technologies de sécurité » remis par MIS (J-M.), vol. I, septembre 2021, 68 p.

Rapport législatif n° 496 de la Commission mixte paritaire, Projet de loi relatif aux jeux Olympiques et Paralympiques de 2024, Compte-rendu intégral des débats du 4 avril 2023.

- **Conseil d'État**

CE, Étude annuelle sur « Le numérique et les droits fondamentaux », 9 septembre 2014.

CE, Étude annuelle 2017 sur « Puissance publique et plateforme numériques : accompagner l'ubérisation », 13 juillet 2017.

CE, Avis n° 401214 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, 20 septembre 2020.

CE, Avis n°404020 du 12 octobre 2021 (non publié).

CE, Étude à la demande du Premier ministre sur « Intelligence artificielle et action publique : construire la confiance, servir la performance », 31 mars 2022, 360 p.

CE, Avis n° 406383 relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, 15 décembre 2022.

- **Cour d'appel de Paris**

Cour d'appel de Paris, Rapport du groupe de travail sur « La réforme du droit français de la responsabilité civile et les relations économiques », avril 2019, 109 p.

- **Autorités administratives indépendantes**

  - **Commission nationale consultative des droits de l'homme (CNCDH)**

CNCDH, Avis sur le projet de loi relatif au renseignement, 16 avril 2015, *JORF* n°0171 du 26 juillet 2015 texte n°43.

CNCDH, Avis sur la proposition de loi relative à la sécurité globale (A - 2020 - 16), 26 novembre 2020, *JORF* n°0289 du 29 novembre 2020.

CNCDH, Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux, 7 avril 2022, *JORF* n°0091 du 17 avril 2022.

  - **Commission nationale informatique et libertés (CNIL)**

CNIL, Délibération n° 94-056 du 21 juin 1994, *15ème rapport d'activité de la Commission nationale de l'informatique et des libertés pour 1994*, éd. La Documentation française, 1995.

CNIL, 24ème Rapport d'activité de 2003, *La Documentation française*, 2004.

CNIL, Délibération n° 2015-255 du 16 juillet 2015, demande d'autorisation n° 1833589.

CNIL, Rapport de synthèse du débat public animé par la CNIL sur les enjeux éthiques des algorithmes et de l'intelligence artificielle « Comment permettre à l'Homme de garder la main ? - Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle », décembre 2017, 80 p.

CNIL, Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports.

CNIL, Délibération n°SAN-2021-003 du 12 janvier 2021 concernant x (anciennement le ministère de l'Intérieur).

CNIL, Délibération n° 2021-011 du 26 janvier 2021 portant avis sur une proposition de loi relative à la sécurité globale, avis n° 20020769.

CNIL, Délibération n°2021-078 du 8 juillet 2021 portant avis sur un projet de loi relatif à la responsabilité pénale et à la sécurité intérieure, avis n° 21012005.

CNIL, « Position sur les conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics », 19 juillet 2022, 18 p.

CNIL, Délibération n° 2022-118 du 8 décembre 2022 portant avis sur un projet de loi portant sur les jeux Olympiques et Paralympiques de 2024, avis n° 22017438.

CNIL, Délibération n° 2023-027 du 16 mars 2023 portant avis sur un projet de décret portant application des articles L. 242-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre de traitements d'images au moyen de dispositifs de captation installés sur des aéronefs par les services de la police nationale, de la gendarmerie nationale, des douanes ainsi que les militaires des armées déployés sur le territoire national dans le cadre des réquisitions prévues à l'article L. 1321-1 du code de la défense, avis n° 22015146.

CNIL, Décision n° MED-2023-018 du 3 avril 2023 mettant en demeure le ministère de l'économie, des finances et de la souveraineté industrielle et numérique.

CNIL, Rapport annuel de 2022 « Agir pour un futur numérique responsable », mai 2023.

- **Défenseur des droits (DDD)**

DDD, Rapport annuel 2011.

DDD, Rapport annuel d'activité 2018.

DDD, Rapport « Technologies biométriques : l'impératif respect des droits fondamentaux », 19 juillet 2019.

DDD, Rapport annuel d'activité 2019.

DDD, Rapport « Algorithmes : prévenir l'automatisation des discriminations », 31 mai 2020.

DDD, avis n°20-05 du 3 novembre 2020 relatif à la proposition de loi sur la sécurité globale.

DDD, avis n°20-06 du 17 novembre 2020 relatif au texte adopté par la commission des lois, sur la proposition de loi relative à la sécurité globale.

DDD, avis n°20-13 du 21 décembre 2020 relatif à la proposition de loi relative à la sécurité globale.

DDD, avis n°21-12 du 20 septembre 2021 relatif au projet de loi sur la responsabilité pénale et la sécurité intérieure.

DDD, Avis établissant des recommandations et des principes essentiels pour la future législation européenne portant sur l'intelligence artificielle : « Pour une IA européenne protectrice et garante du principe de non-discrimination », 21 juin 2022.

DDD, Rapport annuel d'activité 2022.

- **Agence nationale de la sécurité des systèmes d'information (ANSSI)**

ANSSI, Politique de sécurité des systèmes d'information de l'État, (PSSIE) 17 juillet 2014, 42 p.

- **Comité d'études sur la violence, la criminalité et la délinquance**

Rapport dit Peyrefitte à M. le président de la République présenté par le comité d'études sur la violence, la criminalité et la délinquance, 27 juill. 1977, *La documentation française*, 193 p.

- **Conseil économique, social et environnemental (CESE)**

CESE, Rapport sur « Étude d'impact, mieux évaluer pour mieux légiférer » remis par CABRESPINES (J-L.), 2019 (mis à jour le 28 juillet 2020), 90 p.

- **Cour des comptes**

Cour des Comptes, « Rapport public thématique : L'organisation et la gestion des forces de sécurité publique », 7 juillet 2011.

Cour des comptes, Rapport public annuel sur « Amplifier la modernisation numérique de l'État », février 2018.

Cour des comptes, « Rapport : Les polices municipales », octobre 2020.

Cour des comptes, Référé S2021-2194 « Le plan de vidéoprotection de la préfecture de police de Paris » adressé au Ministère de l'Intérieur, 2 décembre 2021.

- **Ministère de la Défense**

Ministère de la Défense, Rapport « Livre blanc sur la défense et la sécurité nationale 2008 » remis par MALLET (J-C.), 17 juin 2008, 402 p.

Ministère de la Défense, Rapport « Livre blanc sur la défense et la sécurité nationale 2013 » remis par GUÉHENNO (J-M.), 29 avril 2013, 160 p.

- **Ministère de l'Écologie, du Développement durable et de l'Énergie**

Direction Générale de l'Aviation Civile (DGAC), Guide « Usages des aéronefs sans équipage à bord : Catégorie spécifique », Édition 1, Version 1.7, 2 mars 2023.

- **Ministère de l'Économie, des Finances et de la Souveraineté Industrielle et Numérique**

Ministère de l'Économie, des Finances et de la Relance, « Rapport - Intelligence artificielle : État de l'art et perspectives pour la France », février 2019.

- **Ministère de l'Intérieur**

Ministère de l'Intérieure, Rapport sur « La cybercriminalité » délivré par BRETON (T.), 1er février 2005, 22 p.

Institut national des hautes études de la sécurité et de la justice (INHESJ), , « La vidéo-protection. Conditions d'efficacité et critères d'évaluation », *IHEMI*, 2008.

Ministère de l'Intérieur, « Rapport sur l'efficacité de la vidéoprotection » émis par SALLAZ (J-P.), DEBROSSE (P.) et HAN (D.), 1er juillet 2009, 82 p.

Ministère de l'Intérieur, « Discours de Gérard COLLOMB - Ouverture des 5ème assises de la sécurité privée », 5 février 2018.

Ministère de l'Intérieur, Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale, 7 juin 2018.

Centre des Hautes Études du Ministère de l'Intérieur (CHEMI), Rapport final sur l'« Encadrement des risques techniques et juridiques des activités de police prédictive » remis par CASTET-RENARD (C.), BESSE (P.), LOUBÈS (J-M.) et PERRUSSEL (L.), 12 juillet 2019, 86 p.

INHESJ, « Anticiper le crime : généalogie, actualité et perspectives », 25 février 2020 [en ligne].

Ministère de l'Intérieur, « Schéma national du maintien de l'ordre », 16 septembre 2020.

Ministère de l'Intérieur, « Livre blanc de la Sécurité intérieure », 16 novembre 2020, 332 p.

- **Ministère de la Justice**

Ministère de la Justice, Rapport sur « La présomption d'innocence : un défi pour l'Etat de droit » remis par GUIGOU (É.), octobre 2021, 217 p.

Textes européens et internationaux :

- **Commission européenne**

Commission européenne, « Lignes directrices en matière d'éthique pour l'IA » remises par le GEHN sur IA de la Commission européenne, 8 avril 2019, 41 p.

Commission européenne, « Livre blanc Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance », 19 février 2020, COM(2020) 65 final, 31 p.

Commission européenne, « Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle et modifiant certains actes législatifs de l'Union) », 21 avril 2021, COM(2021) 206 final.

- **Conseil de l'Europe**

Conseil de l'Europe, « Discrimination, intelligence artificielle et décision algorithmiques », 2018, 99 p.

Conseil de l'Europe, « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ), 3-4 décembre 2018, 84 p.

Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), Lignes directrices sur « L'intelligence artificielle et la protection des données », 25 janvier 2019.

Comité ministériel du Conseil de l'Europe, « Recommandation aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme », CM/Rec(2020)1, 8 avril 2020, 15 p.

Comité *Ad Hoc* sur l'Intelligence artificielle (CAHAI) du Conseil de l'Europe, Étude (2021) sur « Un cadre juridique pour les systèmes d'intelligence artificielle », 17 décembre 2020, 55 p.

Conseil de l'Europe, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), Lignes directrices sur « la reconnaissance faciale », 28 janvier 2021.

- **Conseil de l'Union européenne**

Conseil de l'Union européenne, Rapport n° 13802/1/21 sur l'état des travaux de la proposition de REIA (législation sur l'intelligence artificielle), 22 novembre 2021.

- **Parlement européen**

Parlement européen, Résolution sur « Une politique industrielle européenne globale sur l'intelligence artificielle et la robotique », 12 février 2019 (2018/2088(INI)).

Parlement européen, Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique 2015/2103 (INL).

Parlement européen, « Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes - Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL)) », 20 octobre 2020.

Parlement européen, « Un régime de responsabilité civile pour l'intelligence artificielle - Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle », 20 octobre 2020.

Parlement européen, Résolution sur « L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales », 6 octobre 2021, (2020/2016(INI)), *JOUE* C132/17, 24 mars 2022.

European Parlement,"Draft Compromise Amendments - Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts", May 9th 2023, 144 p.

Parlement européen, P9_TA(2023)0236 Législation sur l'intelligence artificielle, 14 juin 2023.

- **Agence Européenne de la Sécurité Aérienne (AESA/*EASA*)**

EASA, Advance Notice of Proposed Amendment (A-NPA) 2015-10 - Introduction of a regulatory framework for the operation of drones, 31 July 2015, 41 p.

- **Comité Européen de Protection des Données (CEPD/*EDPB*) et G29**

G29, Avis 05/2014 sur les Techniques d'anonymisation, 10 avril 2014, 42 p.

G29, Avis n° 01/2015 sur la vie privée et les problématiques de données personnelles au regard de l'utilisation des drones du 16 juillet 2015, 21 p.

G29, « Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 », 3 octobre 2017 (version révisée du 6 février 2018).

EDPB-EDPS, "Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection", July 12th 2019.

EDPB, « Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo », Version 2.0, 29 janvier 2020, 35 p.

EDPB, Recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif, 2 février 2021, v. 1, 19 p.

EDPB, Avis conjoint 05/2021 de l'EDPB et du CEPD sur « la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) », 18 juin 2021.

EDPB, « EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination », June 21st 2021.

EDPB, « Overview on resources made available by Member States to the Data Protection Supervisory Authorities », September 5th 2022.

- **Conseil des barreaux européens (CCBE)**

CCBE, « Considérations du CCBE sur les aspects juridiques de l'intelligence artificielle », Bruxelles, 2020, 42 p.

- **European Union Agency for Fundamental Rights (FRA)**

FRA, Report on "Bias in algorithms - artificial Intelligence and Discrimination", Vienna, December 8th 2022.

- **Irish Council for Civil Liberties (ICCL)**

ICCL, ICCL's 2023 report on EEA data protection authorities, May 31st 2023.

- **Organisation des Nations Unies (ONU)**

ONU (Conseil des droits de l'homme), Commentaires et suggestions à propos de la proposition de loi n° 3452 relative à la sécurité globale datant du 20 octobre 2020, 12 novembre 2020.

- **Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO)**

UNESCO, « Recommandation sur l'éthique de l'intelligence artificielle », 2022, 43 p.

- **Organisation du Traité de l'Atlantique Nord (OTAN)**

NATO, Tallin Manual 2.0 on the International Law Applicable to Cyber Operations, 2017, 215 p.

VI. Guides méthodologiques et référentiels

AFNOR, Guide AFNOR BP Z90-001 « Prévention et gestion de la fuite d'information : Référentiel de bonnes pratiques », décembre 2014 [en ligne].

AFNOR, Normes IA « Grand Défi IA » [en ligne].

ANSSI, « Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) : Méthode de gestion des risques », 25 janvier 2010 [en ligne].

ANSSI, « Recommandations de sécurité n°524/ANSSI/SDE pour la mise en oeuvre de dispositifs de vidéoprotection », 14 février 2013 [en ligne].

ANSSI, « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection - v2.0 », 4 mars 2020 [en ligne].

ANSSI, « EBIOS Risk Manager (EBIOS RM) : Méthode d'appréciation et de traitement des risques numériques », 26 juillet 2022 [en ligne].

ANSSI, Guide « Les mesures cyber préventives prioritaires », 3 mai 2023 [en ligne].

CNIL, « Guide de la sécurité des données personnelles » dont la dernière version date du 3 avril 2023 [en ligne].

Laboratoire national de métrologie et d'essais (LNE), « Référentiel de certification de processus pour l'IA », 2021 [en ligne].

Syndicat professionnel des entreprises du numérique en France (Numeum), Guide pratique « Ethical IA », septembre 2021 [disponible en ligne].

VII. Ressources informatiques, liens internet consultés et articles de presse

« La Russie impliquée dans la cyber-attaque contre l'Estonie ? », *journaldunet.com*, 1er juin 2007 [en ligne].

« Les 10 plus grandes manifestations en France depuis 15 ans », *Le Nouvel Obs*, 8 septembre 2010 [en ligne].

"Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, June 11th 2013 [en ligne].

« Détournement des caméras de vidéo-surveillance en botnet », *Undernews*, 4 novembre 2015 [en ligne].

« Euro 2016, la Police renforce sa flotte de drones de surveillance », *Robots & cie*, 10 mai 2016 [en ligne].

"Community Control Over Police Surveillance: Technology 101", *ACLU*, September 16th 2016 [en ligne].

« Sécurité routière : les drones policiers ne font pas tomber les PV du ciel », *AFP*, 7 octobre 2016 [en ligne].

« Incendies : cinq innovations pour lutter contre les feux de forêt », *France Info*, 25 juillet 2017 [en ligne].

« Les policiers obtiennent une revalorisation salariale après une journée de protestation », *Journal du Dimanche*, 20 décembre 2018 [en ligne];

« Les syndicats de policiers obtiennent une revalorisation salariale », *ladepeche.fr*, 20 décembre 2018 [en ligne].

« Fronde des policiers : un accord de revalorisation salariale a été conclu entre Castaner et les syndicats », *europe1.fr*, 20 décembre 2018 [en ligne].

« Les libertés fondamentales "en très mauvais état" en France, s'inquiète le président de la CNCDH », *Lamy Actualité du Droit*, 29 avril 2019.

« Le nombre de policiers et gendarmes blessés en mission a augmenté de 15 % en 2018 », *Le Monde*, 7 novembre 2019 [en ligne].

« St Etienne : des capteurs sonores à l'écoute de la ville », 1er mars 2019 [en ligne].

« Le vrai visage de la reconnaissance faciale », *La Quadrature du Net*, 21 juin 2019 [en ligne].

« L'intelligence artificielle au service de la cybersécurité », *IA Data Analytics*, 23 janvier 2020 [en ligne].

« 20 MINUTES AVEC... » Jacques Toubon, *20minutes.fr*, 12 juin 2020 [en ligne].

« À la veille de son départ, le Défenseur des droits encourage les Français à saisir l'institution », *Le Figaro*, 1er juillet 2020 [en ligne].

« Drones en manifestation : La Quadrature contre-attaque », *La Quadrature du Net*, 26 octobre 2020 [en ligne].

« France. La nouvelle loi sur la sécurité globale risque d'instaurer une surveillance d'État démesurée et inacceptable », *Amnesty International*, 3 mars 2021 [en ligne].

« Sécurité globale : le Sénat dit oui à la surveillance de masse », *La Quadrature du Net*, 19 mars 2021 [en ligne].

« La panne des numéros d'urgence causée par un « bug » logiciel, selon l'enquête interne d'Orange », *Le Monde*, 11 juin 2021 [en ligne].

« Le renseignement russe avait piraté la police néerlandaise », *NextInpact*, 18 juin 2021 [en ligne].

« Les drones policiers autorisés par le Conseil constitutionnel », *La Quadrature du Net*, 21 janvier 2022 [en ligne].

« Adversarial Attack : Définition et protection contre cette menace », *Datascientest*, 4 mars 2022 [en ligne].

« Cloud de la DGSI : Atos ou Thales pour succéder à Palantir ? », *Siècle Digital*, 3 janvier 2023 [en ligne].

« Non à la vidéosurveillance algorithmique, refusons l'article 7 de la loi olympique », *La Quadrature du Net*, 18 janvier 2023 [en ligne].

« Les mesures de vidéosurveillance algorithmique introduites par la loi JO 2024 sont contraires au droit international », *Le Monde*, 7 mars 2023 [en ligne].

« 35 organisations internationales demandent le retrait de l'article 7 du projet de loi JO 2024 », *NextInpact*, 7 mars 2023 [en ligne].

"European Parliament: Make sure the AI act protects peoples' rights!", April 2023 [en ligne].

"Biometric Surveillance Is Quietly Expanding: Bright-Line Rules Are Key", *AI Now Institute*, April 11th 2023 [en ligne].

« Les outils d'IA sont utilisés par la police qui « ne comprend pas comment ces technologies fonctionnent », selon une étude de l'Université d'État de Caroline du Nord », *développez.com*, 17 mai 2023 [en ligne].

« Comment l'IA va bouleverser la cybersécurité ? », *Le Big Data*, 30 mai 2023 [en ligne].

« Pour Thierry Breton, la régulation des IA est analogue au permis de conduire », *NextInpact*, 20 juin 2023 [en ligne].

« Le vol à l'étalage fait le lit de la vidéosurveillance algorithmique », *NextInpact*, 28 juin 2023 [en ligne].

« Cloud : 1,2 milliard d'euros pour un Projet important d'intérêt européen commun », *Next Ink*, 8 décembre 2023 [en ligne].

« Archives des manifestations de France 24 », *france24.com* [en ligne].

ALLARD (T.), Dossier sur « IA - L'intelligence artificielle pourra-t-elle un jour remplacer les politiques ? », *Sciences & Vie* n° 1255, avril 2022, pp. 64-81.

Alliance pour la confiance numérique (ACN) a contribué à l'élaboration d'une charte éthique de la profession [en ligne].

ANSSI, « Management du risque : obsolescence de la méthode EBIOS 2010 », 26 juillet 2022 [en ligne] consulté le 26 juillet 2022.

AUCLERT (F.), « Et si le « deepfake » contaminait les images satellites », *Futura Tech*, 23 avril 2021 [en ligne].

BADINTER (R.), « On tombe dans la répression administrée et on ouvre la voie à tous les soupçons », *Le Monde*, 27 janvier 2004 [en ligne].

BARTHE (O.), « Icarus, le boîtier capable de pirater les drones », *lemondeinformatique.fr*, 28 octobre 2016 [en ligne].

BASCOU (S.), « Cyberattaques : en quoi consiste le « bouclier cybereuropéen » voulu par l'UE ? », *01net*, 5 avril 2023 [en ligne].

BENSOUSSAN (A.), « Plaidoyer pour un droit des robots : la "personne morale" à la "personne robot" », *La Lettre des juristes d'affaires*, 23 octobre 2013, n° 1134.

BERNARD (P.), « Des drones pour sécuriser Marseille, une idée qui séduit », *Le Figaro*, 19 septembre 2013 [en ligne].

BIGET (S.), « Le site de l'Assemblée nationale mis K.-O. par des hackers russes », *Futura Sciences*, 27 mars 2023 [en ligne].

BISEUL (X.), « Comment se prémunir contre les attaques d'objets connectés « zombies » », *Journal du net*, 23 novembre 2016 [en ligne].

BODNAR (B.), « Des hackers russes s'attaquent à la France pendant le discours de Poutine », *Numerama*, 21 février 2023 [en ligne].

BODNAR (B.), « Le site de l'Assemblée nationale en panne après une cyberattaque de hackers russes », *Numerama*, 27 mars 2023 [en ligne].

BRANDELA (H.), « Fichier SIRENE et non-conformité à la loi Informatique et Libertés », *Village de la Justice*, 29 mai 2023 [en ligne].

BRIGGS (E.), "The AI Frenzy Is Introducing Marketing Buzzwords That Consumers Don't Understand", *Morning Consult*, April 24th 2023 [en ligne].

BROOKS (R.), « Pourquoi l'intelligence artificielle nous fait autant fantasmer », *Courrier international*, 20 décembre 2017 [en ligne].

BRUMFIELD (C.), « 5 ans après, quelles leçons tirer des attaques NotPetya », *Lemondeinformatique*, 4 juillet 2022 [en ligne].

BULLINGTON (J.) and LANE (E.), "New Orleans ends its relationship with tech firm Palantir, Landrieu's office says", *NOLA.com | The Times-Picayune*, March 14th 2018 (updated on July 12th 2019) [en ligne].

CEDH, Fiche thématique « Nouvelles technologies » [en ligne].

CHARTIER (M.), « Project Maven : le Pentagone signe pour 50 millions de dollars de contrats avec Amazon et Microsoft », *Les Numériques*, 9 septembre 2021 [en ligne].

CHAUVIN (H.), « JO 2024 : la France championne de la surveillance de masse », *Reporterre*, 27 janvier 2023 [en ligne].

CHEMINAT (J.), « L'accès au code source d'un logiciel d'analyse d'ADN à la barre », *Le Monde Informatique*, 5 février 2021 [en ligne].

CHEMINAT (J.), « Le ministère de l'Intérieur lance le chantier de son futur réseau radio 4G/5G », *Le Monde Informatique*, 14 octobre 2022 [en ligne].

CIMINO (V.), « Piratage SolarWinds : les hackers ont eu accès aux e-mails du DHS (Department of Homeland Security) », *Siècle Digital,* 30 mars 2021 [en ligne].

CIMINO (V.), « Le futur règlement européen sur l'intelligence artificielle peut-il être un frein à l'innovation ? », *Siècle Digital*, 18 novembre 2021 [en ligne].

CLAVEY (M.), « La CNIL étrille le fichier illégal SIRENE de la douane maritime », *Next Inpact*, 21 avril 2023 [en ligne].

CNIL, « Vidéosurveillance / vidéoprotection : les bonnes pratiques pour des systèmes plus respectueux de la vie privée », 21 juin 2012 [en ligne].

CNIL, « Drones, innovations, vie privée et libertés individuelles », *La lettre Innovation et Prospective*, n°6, décembre 2013 [en ligne].

CNIL, « La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo », 19 septembre 2018 [en ligne].

CNIL, Lettre de la présidente de la CNIL au président de Saint-Étienne métropole le 25 octobre 2019 [en ligne].

CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », 29 octobre 2019 [en ligne].

CNIL, « Reconnaissance faciale - Pour un débat à la hauteur des enjeux », 15 novembre 2019, 11 p. [en ligne].

CNIL, « La vidéosurveillance – vidéoprotection sur la voie publique », 3 décembre 2019 [en ligne].

CNIL, « Identifier les données personnelles », 27 janvier 2020 [en ligne].

CNIL, « Suspension de l'utilisation des drones pour contrôler le déconfinement à Paris par le Conseil d'État : les contrôles de la CNIL », 18 mai 2020 [en ligne].

CNIL, « La CNIL appelle à la vigilance sur l'utilisation des caméras dites « intelligentes » et des caméras thermiques », 17 juin 2020 [en ligne].

CNIL, « La CNIL rend son avis sur la proposition de loi "sécurité globale" », 3 février 2021 [en ligne].

CNIL, « Audition devant la Commission des lois du Sénat dans le cadre de l'examen de la proposition de loi relative à la sécurité globale », 3 février 2021 [en ligne].

CNIL, « Intelligence artificielle : l'avis de la CNIL et de ses homologues sur le futur règlement européen », 8 juillet 2021 [en ligne].

CNIL, « Fichier automatisé des empreintes digitales : rappel à l'ordre du ministère de l'Intérieur », *cnil.fr*, 30 septembre 2021 [en ligne].

CNIL, « Intelligence artificielle, de quoi parle-t-on ? », *cnil.fr*, 25 mars 2022 [en ligne].

CNIL, « Jeux olympiques et paralympiques 2024 : la CNIL publie son avis sur le projet de loi », *cnil.fr*, 4 janvier 2023 [en ligne].

CNIL, « Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage », *cnil.fr*, 23 janvier 2023.

CNIL, « Thématiques prioritaires de contrôle 2023 : caméras « augmentées », applications mobiles, fichiers bancaires et dossiers patients », *cnil.fr*, 15 mars 2023 [en ligne].

CNIL, « La France ratifie la Convention 108+ du Conseil de l'Europe », *cnil.fr*, 30 mars 2023 [en ligne].

CNIL, « L'usage des drones par les forces de l'ordre », 27 avril 2023 [en ligne].

CNIL, « La CNIL met en demeure le ministère de l'Économie de régulariser un fichier utilisé par les douanes », *cnil.fr*, 29 mai 2023 [en ligne].

Communication de la Commission au Conseil et au Parlement européen, « La Création du ciel unique européen », COM(1999) 614 final, 1er décembre 1999, 39 p. [en ligne].

CONGER (K.) and CAMERON (D.), "Google Is Helping the Pentagon Build AI for Drones", *gizmodo.com*, March 6th 2018 [en ligne].

Conseil constitutionnel, « Les droits et libertés » [en ligne].

COURMONT (A.) et SALIOU (J.), « Comment la vidéosurveillance vient au village ? », *linc.cnil.fr*, 19 novembre 2021 [en ligne].

CORNEVIN (C.), « Les gendarmes déploient leurs drones », *Le Figaro*, 3 février 2016 [en ligne].

CROCHET-DAMAIS (A.), « Inférence en machine learning et deep learning : définition et cas d'usage », *Journal du Net*, 8 mars 2022 [en ligne].

CROUZILLACQ (P.), « L'Estonie dénonce les cyber-attaques terroristes russes », *01net.com*, 11 juin 2007 [en ligne].

CURRIER (C.), MOLTKE (H.), "Spies in the sky. Israeli drone feeds hacked by British and American Intelligence", *The Intercept*, 29 January 2016 [en ligne].

Cybersecurity & Infrastructure Security Agency (CISA), "FBI Releases PIN on Ransomware Straining Local Governments and Public Services", March 31st 2022 [en ligne].

DELACROIX (F.), « Comprendre les algorithmes numériques », *InterCDI 273*, mai - juin 2018 [en ligne].

DELUZARCHE (C.), « Un nouveau type de cyberattaque qui fait bondir la consommation énergétique de l'IA », *Futura Sciences*, 11 mai 2021 [en ligne].

DESTAL (M.), LE FOLL (C.) et LIVOLSI (G.) « La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale », *Disclose*, 14 novembre 2023 [en ligne].

EDRi, « Surveillance and data retention » [en ligne].

EDRi (European Digital Rights), "Civil society urges European Parliament to protect people's rights in the AI Act", April 9th 2023 [en ligne].

ESTIMBRE (T.), « La surveillance de masse par drones policiers devient légale en France », *journal du geek*, 25 janvier 2022 [en ligne].

European Center for Not-for-profit Law (ECNL), « Lettre de la société civile sur le projet de loi relatif aux Jeux olympiques et paralympiques 2024 », *ecnl.org*, 7 mars 2023 [en ligne].

European Parlement, Press release "AI Act: a step closer to the first rules on Artificial Intelligence", May 11th 2023 [en ligne].

Fablex DL4T, Rapport sur « Les usages européens de la reconnaissance faciale », avril 2020 [en ligne].

FÉRAL-SCHUHL (C.) et SINIBALDI (J.), « Un cadre juridique européen pour l'intelligence artificielle : une première mondiale ! », *feral.law*, 15 novembre 2021 [en ligne].

FRANCESCANI (C.), "NYPD expands surveillance net to fight crime as well as terrorism", *Reuters*, June 21st 2013 [en ligne].

FRIEDERSDORF (C.), "A Police Department's Secret Formula for Judging Danger", *The Atlantic*, January 13th 2016 [en ligne].

GAVOIS (S.), "Gaia-X « vit toujours » et « arrive à des étapes très concrètes » », *Next Ink*, 4 décembre 2023 [en ligne].

Gendarmerie nationale, « La Gendarmerie, de l'analyse prédictive à l'analyse décisionnelle », *L'essor de la gendarmerie nationale*, 26 janvier 2018 [en ligne].

GORMAN (S.), DREAZEN (Y. J.), COLE (A.), "Insurgents hack US Drones", *Wall Street Journal*, 17 December 2009 [en ligne].

GREENBERG (A.), "The Untold story of notpetya, the most devastating cyberattack in history", August 22nd 2018 [en ligne].

GUILLERMARD (V.), « L'armée investit pour lutter contre les cybermenaces », *Le Figaro*, 6 juin 2014 [en ligne].

HAWKING (S.), « L'intelligence artificielle pourrait mettre fin à l'humanité », *Le Monde et AFP*, 3 décembre 2014 [en ligne].

HOAREAU (C.), « Drones et lutte contre les feux de forêt : la connectivité, nerf de la guerre », *Journal du Net*, 13 décembre 2021 [en ligne].

Human Rights Watch, « France : Rejeter la surveillance dans la loi sur les Jeux Olympiques 2024 - Un système de surveillance basé sur des algorithmes violerait les droits fondamentaux », *hrw.org*, 7 mars 2023 [en ligne].

IFOP, « Notoriété et image de l'intelligence artificielle auprès des Français et des salariés », *ifop.com*, 28 janvier 2021 [en ligne].

IFRAH (L.), « Analyse de la première attaque massive des systèmes d'information d'un Etat », *Revue Défense Nationale* n°700, septembre 2007, pp. 104-114 [en ligne].

IKONICOFF (R.), « Et la machine se mit à penser », *Sciences & Vie* Hors Série n° 290, mars 2020, pp. 8-15, spéc. pp. 12-13.

Impervia, « CCTV DDoS Botnet In Our Own Back Yard », 21 October 2015 [en ligne].

INSEE, Première, n° 1780, 30 octobre 2019 [en ligne].

JEAN (A.), « Transparence et explicabilité des algorithmes, la grande confusion », *lepoint.fr*, 13 juin 2021 [en ligne].

JOSEPH (G.) and LIPP (K.), "IBM used NYPD surveillance footage to develop technology that lets Police Search by Skin Color", *The Intercept_*, September 6th 2018 [en ligne].

JUSQUIAME (T.), « Ils utilisent la surveillance algorithmique : Leclerc, Fnac, Biocoop et de nombreux commerces surveillent illégalement leurs clients », *Street Press*, 27 juin 2023 [en ligne].

KARAYAN (R.), « Coup d'envoi pour le "réseau radio du futur", opérationnel en 2024 », *L'Usine Digitale*, 13 octobre 2022 [en ligne].

La Quadrature du Net, « Technopolice » [en ligne].

La Quadrature du Net, « Vidéosurveillance biométrique dans nos supermarchés », *laquadrature.net*, 31 mai 2021 [en ligne].

LARSON (J.), ANGWIN (J.), MATTU (S.) and KIRCHNER (L.), "Machine Bias", *ProPublica*, May 23rd 2016 [En ligne].

LECHENET (A.), « La vidéosurveillance dans le viseur de la Cour des comptes », *La Gazette des communes*, 26 octobre 2020 [en ligne].

LE FOLL (C.) et POURÉ (C.), « Avec le confinement, les drones s'immiscent dans l'espace public », *Médiapart*, 25 avril 2020 [en ligne].

LE FOLL (C.) et POURÉ (C.), « Profitant du flou juridique, les drones policiers bourdonnent toujours », *Médiapart*, 26 octobre 2020 [en ligne].

LE FOLL (C.) et POURÉ (C.), « Thales à Roland-Garros : têtes et match », *Les Jours*, 9 novembre 2021 [en ligne].

LE NEVÉ (S.), « La justice prépare sa révolution algorithmique », *Acteurs Publics*, 27 juin 2017 [en ligne].

Les archives du ministère de l'Intérieur [en ligne].

LINC-CNIL, Cahier IP n° 5 « La plateforme d'une ville - Les données personnelles au coeur de la fabrique de la smart city », *linc.cnil.fr,* septembre 2017, p. 39 [en ligne].

LINC-CNIL, « Dossier - Sécurité des systèmes d'IA » rédigé par VALLET (F.), *linc.cnil.fr*, avril 2022 [en ligne].

MACKEY (A.) and MAAS (D.), "Tattoo Recognition Research Threatens Free Speech and Privacy", *Electronic Frontier Foundation* (EFF), June 2nd 2016 [en ligne].

MAINGUET (M.), « Combien de policiers et de gendarmes tués en mission en France ? », *Ouest-France*, 11 mai 2021 [en ligne].

MARIN (J.), « La police et l'armée suisses victimes collatérales d'une cyberattaque », *Usine Digitale*, 5 juin 2023 [en ligne].

MAZHAR (S.), « Intelligence artificielle : Le G7 travaille sur une "utilisation responsable" », *ladepeche.fr*, 22 mai 2023 [en ligne].

Mc CARTHY (S.), ZHENG (W.) and TSANG (D.), "HK$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show", *South China Morning Post*, 29 October 2018 [en ligne].

Mc CULLAGH (D.), "U.S Was Warned of Predator drone Hacking", *CBS News*, 17 December 2009 [en ligne].

Mc DONALD (B.), « L'Union européenne en passe de devenir un leader mondial dans l'IA éthique », *journaldunet.com*, 9 mars 2023 [en ligne].

Mc GUIRE (M.), "Nation States, Cyberconflict and the Web of Profit", University of Surrey, April 2021 [en ligne].

MICK (J.), "Iran: Yes We Hacked the U.S's Drone and Here's How we Did It", *Daily Tech*, 15 December 2011 [en ligne].

MILLON (L.), « Comment la police française exploite le potentiel des drones », *Siècle digital*, 17 novembre 2017 [en ligne].

Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, « Panne des numéros d'urgence : le Gouvernement annonce des premières mesures », 22 juillet 2021 [en ligne].

MODDERKOLK (H.), « Russen zaten ten tijde van mh17 onderzoek door hack diep in systemen politie », *Volkskrant*, 8 juin 2021 [en ligne].

MONNIER (E.), « Un premier drone militaire décolle en France », *Science et Vie* n°1198, juillet 2017, pp. 128-130.

MUELLER (B.), "The Artificial Intelligence Act Is a Threat to Europe's Digital Economy and Will Hamstring The EU's Technology Sector In The Global Marketplace", *Center for Data Innovation*, April 21st 2021 [en ligne].

NAKASHIMA (E.), "At nations' request, US Cyber Command probes foreign networks to hunt election security threats", *Washington Post*, 7 May 2019 [en ligne].

National Intelligence Council, "Structural Forces - Technology", March 2021, 65 p. p. 63 [en ligne].

NICHOLS (G.), "Cheap GPS jammers a major threat to drones", *zdnet.com*, 14 December 2020 [en ligne].

NIKITINE (K.), « Mathématiques : À la recherche du meilleur des mondes », *Sciences & Vie* n° 1260, septembre 2022, pp. 98-101.

NIST, "Tattoo Recognition Technology", July 13th 2017 [en ligne].

NORMAND (J-M.), « Les drones, nouvel outil contre les incendies de forêt », *Le Monde*, 12 août 2016 [en ligne].

Observatoire national de la délinquance et des réponses pénales (ONDRP), Note n°39 sur « Les policiers et gendarmes décédés et blessés en 2018 » par SOULLEZ (C.), novembre 2019 [en ligne].

ONERA, « Mieux connaître les drones », 48 p. [en ligne].

ONU, « Urgent action needed over artificial intelligence risks to human rights », 15 September 2021 [en ligne].

PALMER (D.), « Aux Etats-Unis, les ransomwares s'attaquent aux services publics », *ZDNet*, 1er avril 2022 [en ligne].

PINTE (J-P.), Blog « Cyberisques, cybercriminalité et nouveau monde » [en ligne].

Président Jean-Claude Juncker, « Discours sur l'état de l'Union 2017 », Bruxelles, 13 septembre 2017 [en ligne].

RICHARDSON (R.), "Community Forum on Algorithmic Bias", *AI Now Institute*, December 7th, 2019 [en ligne].

RIGAKI (M.) and GARCIA (S.), "A Survey of Privacy Attacks in Machine Learning", April 1st 2021 [en ligne].

RIMBOT (A.), « Hébergement de la data en France : un devoir de souveraineté numérique », *appvizer*, 20 décembre 2022 [en ligne].

ROCHERFORT (M.), « Des chercheurs alertent sur l'émergence des deepfakes d'images par satellite », *Siècle Digital*, 28 avril 2021 [en ligne].

ROCHEFORT (M.), « Des chercheurs alertent sur une nouvelle forme de hack visant les IA », *Siècle Digital,* 7 mai 2021 [en ligne].

ROCHEFORT (M.), « La demande en datacenters boostée par la souveraineté des données », *Siècle Digital*, 4 août 2023 [en ligne].

ROLLAND (S.) et MABILLE (P.), Interview de Jean-Noël Barrot, ministre de la Transition numérique « Non, il ne faut pas interdire ChatGPT », *La Tribune*, 6 avril 2023 [en ligne].

ROSEMAIN (M.), « La DGSI renouvelle son contrat avec l'Américain Palantir, faute de système 100 % français », *L'Usine Digitale*, 27 novembre 2019 [en ligne].

RUIZ (P.), « Le développement de l'IA sans réglementation induit une menace existentielle pour l'humanité », *developpez.com*, 17 février 2023 [en ligne].

SADAUNE (M.), « Utilisation et efficacité professionnelle des drones par les sapeurs-pompiers », pompiers.*fr*, 12 octobre 2017 [en ligne].

Sapeurs-pompiers de France, « Moyens aériens de la Sécurité civile et des sapeurs-pompiers », [en ligne].

Sciences Po (Cevipof), « En qu(o)i les Français ont-ils confiance aujourd'hui ? », *Le baromètre de la confiance politique - vague 13b*, juin 2022, [en ligne].

SERGENT (D.), « Des drones innovants pour lutter contre les feux de forêts », *La Croix*, 6 août 2019 [en ligne].

SERMONDADAZ (S.), « Projet Maven : Google met fin à son partenariat avec le Pengatone américain », *Sciences et Avenir*, 6 juin 2018 [en ligne].

SERRES (M.), « La peur », *France info*, 4 novembre 2012 [en ligne].

SEYDTAGHIA (A.), « Une cyberattaque hors norme frappe la Suisse, touchant l'armée et de nombreuses polices », *Le Temps*, 2 juin 2023 [en ligne].

SGDSN, « Anticiper les risques et les menaces », 22 novembre 2022 [en ligne].

SHACHTMAN (N.), "Computer Virus Hit U.S. Drone Fleet", *Wired*, 17 July 2011 [en ligne].

SIMON (P.), « Notre-Dame-des-Landes, comment les gendarmes ont utilisé des drones », *Ouest France*, 25 juillet 2018 [en ligne].

SLAMA (S.), « Censure partielle de la loi « sécurité globale » : après demain les drones ? », *Leclubdesjuristes.com*, 10 juin 2021 [en ligne].

SMIALOWSKI (B.), « Le G7 établit un protocole sur l'IA pour lutter contre la désinformation », *i24news*, 20 mai 2023 [en ligne].

SMITH (M.), "Beware: Surveillance software police are using to score citizens' threat level", *CSO*, January 11th 2016 [en ligne].

STANLEY (J.), "The Dawn of Robot Surveillance - AI, Video Analytics, and Privacy", *American Civil Liberties Union* (ACLU), June 17th 2019 [en ligne].

SUDERMAN (A.), "SolarWinds hack got emails of top DHS officials", *AP News*, 29 March 2021 [en ligne].

Syndicat de la magistrature, « Observations sur le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure - Volet n°3 : dispositions relatives à la surveillance (Articles 7, 8, 9) », *syndicat-magistrature.fr*, 21 septembre 2021 [en ligne].

THIERRY (G.) « Ce que le « réseau radio du futur » va changer pour les sapeurs-pompiers », *La Gazette des communes*, 12 décembre 2022 [en ligne].

TREILLES (C.), « Gaia-X : Le hub français invite les volontaires à rejoindre ses rangs », *zdnet.fr*, 25 janvier 2021 [en ligne].

TRUJILLO (E.), « Panne des numéros d'urgence: la responsabilité d'Orange risque-t-elle d'être engagée ? », *Le Figaro*, 3 juin 2021 [en ligne].

UIT, « Présentation générale de la cybersécurité », 18 avril 2008 [en ligne].

UNESCO, « UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence », 25 November 2021 [en ligne].

VALDENAIRE (L.), « Drones et hélicoptères : les gendarmes du Grand Est déploient les grands moyens pendant le confinement », *France Bleu*, 10 avril 2020 [en ligne].

VALLET (F.), « Philippe Besse : Les décisions algorithmiques ne sont pas plus objectives que les décisions humaines, *linc.cnil.fr*, 2 juin 2020 [en ligne].

Vie publique, « Panne des numéros d'urgence : quelle responsabilité de l'opérateur Orange ? », 29 juillet 2021 [en ligne].

VINCENT (J.), "IBM secretly used New York's CCTV cameras to train its surveillance software", *The Verge*, September 6th 2018 [en ligne].

VITARD (A.), « Le Ministère de la Justice victime d'un ransomware ? », *Usine Digitale*, 28 janvier 2022 [en ligne].

VLASOV (A.) et BARBARINO (M.), « Sept contributions de l'IA au progrès de la science et de la technologie nucléaires », *Agence internationale de l'énergie atomique*, 2 décembre 2022 [en ligne].

WAWRZYNIAK (R.), « Les nouveaux yeux du secours », *Archives des dossiers du Ministère de l'Intérieur*, 22 janvier 2016 [en ligne].

WINSTON (A.), "Palantir has secretly been using New Orleans to test its predictive policing technology", *The Verge*, February 27th 2018 [en ligne].

ZAFFAGNI (M.), « Icarus, le boîtier qui peut pirater n'importe quel drone en plein vol », *futura-sciences.com*, 3 novembre 2016 [en ligne].

ZAPPI (S.), « À Marseille, des élus PS parlent de drones pour lutter contre le crime », *Le Monde*, 24 septembre 2013 [en ligne].

VIII. Multimédia (documentaires, entretiens, visioconférences et webinaires)

ARTE THEMA, « Prédire les crimes », *ARTE*, 2017, diffusé le 2 octobre 2018 [Documentaire disponible en ligne].

ARTE, « Algorithmes - Vers un monde manipulé », *arte.tv*, 2022, diffusé le 11 avril 2023 [Documentaire].

BERTRAND (B.), « Encadrement des technologies de surveillance : les enseignements de l'expérimentation des JO 2024 », 22 mars 2023 [Visioconférence en ligne].

CNIL, « Caméras "augmentées" dans les espaces publics », 23 mai 2023 [Webinaire en ligne].

INHESJ, « Anticiper le crime : généalogie, actualité et perspectives », 25 février 2020 [Conférence en ligne].

LE CUN (Y.), « Qu'est-ce que l'intelligence artificielle », *Le Point*, 16 mars 2017 [vidéo en ligne].

McCABE (D.), "NOVA : Prediction by the Numbers" [2018], 52 min [Documentaire sur Netflix].

PARROT (K.) et ELMADJIAN (S.), Film « Sécurité globale, de quel droit ? », 29 janvier 2021 [disponible en ligne].

Episode #376 « Sécurité des drones », *nolimitsecu.fr*, 17 juillet 2022 [Podcast en ligne].

« Cybersécurité des drones : entretien avec Victor Vuillard, CSO et CTO cybersecurité de Parrot », *InCyber*, 22 novembre 2022 [vidéo en ligne].

TABLE DES DÉCISIONS CITÉES

I. Décisions de l'ordre juridique français

A. Conseil constitutionnel

C. const., Décision n° 62-20 DC, 6 novembre 1962, *Loi relative à l'élection du Président de la République au suffrage universel direct, adoptée par le référendum du 28 octobre 1962*.

C. const., Décision n° 71-44 DC du 16 juillet 1971, *Loi complétant les dispositions des articles 5 et 7 de la loi du 1er juillet 1901 relative au contrat d'association*.

C. const., Décision n° 73-51 DC, 27 décembre 1973, *Loi de finances pour 1974*.

C. const., Décision n° 74-54 DC du 15 janvier 1975, *Loi relative à l'interruption volontaire de la grossesse*.

C. const., Décision n° 76-75 DC, 12 janvier 1977, *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales*.

C. const., Décision n° 79-107 DC, 12 juillet 1979, *Loi relative à certains ouvrages reliant les voies nationales ou départementales*.

C. const., Décision n° 79-105 DC, 25 juillet 1979, *Loi modifiant les dispositions de la loi n° 74-696 du 7 août 1974 relatives à la continuité du service public de la radio et de la télévision en cas de cessation concertée du travail*.

C. const., Décision n° 79-109 DC, 9 janvier 1980, *Loi relative à la prévention de l'immigration clandestine*.

C. const., Décision n° 80-127 DC, 20 janvier 1981, *Loi renforçant la sécurité et protégeant la liberté des personnes*.

C. const., Décision n° 82-141 DC, 27 juillet 1982, *Loi sur la communication audiovisuelle*.

C. const., Décision n° 83-164 DC, 29 décembre 1983, *Loi de finances pour 1984*.

C. const., Décision n° 85-187 DC, 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie et dépendances*.

C. const., Décision n° 86-207 DC, 26 juin 1986, *Loi autorisant le Gouvernement à prendre diverses mesures d'ordre économique et social*.

C. const., Décision n° 86-213 DC, 3 septembre 1986, *Loi relative à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État*.

C. const., Décision n° 86-224 DC, 23 janvier 1987, *Loi transférant à la juridiction judiciaire le contentieux des décisions du Conseil de la concurrence.*

C. const., Décision n° 87-237 DC, 30 décembre 1987, *Loi de finances pour 1988*.

C. const., Décision n°88-244 DC, 20 juillet 1988, *Loi portant amnistie*.

C. const., Décision n° 88-248 DC, 17 janvier 1989, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*.

C. const., Décision n° 89-257 DC, 25 juillet 1989, *Loi modifiant le code du travail et relative à la prévention du licenciement économique et au droit à la conversion*.

C. const., Décision n° 89-260 DC, 28 juillet 1989, *Loi relative à la sécurité et à la transparence du marché financier*.

C. const., Décision n° 89-261 DC, 28 juillet 1989, *Loi relative aux conditions de séjour et d'entrée des étrangers en France*.

C. const., Décision n° 91-294 DC, 25 juillet 1991, *Loi autorisant l'approbation de la convention d'application de l'accord de Schengen du 14 juin 1985*.

C. const., Décision n° 92-307 DC, 25 février 1992, *Loi portant modification de l'ordonnance n° 45-2658 du 2 novembre 1945 modifiée relative aux conditions d'entrée et de séjour des étrangers en France*.

C. const., Décision n° 93-323 DC, 5 août 1993, *Loi relative aux contrôles et vérifications d'identité*.

C. const., Décisions n° 93-326 DC, 11 août 1993, *Loi modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme du code de procédure pénale.*

C. const., Décision n° 93-325 DC, 13 août 1993, *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France*.

C. const., Décision n° 93-333 DC, 21 janvier 1994, *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*.

C. const., Décision n° 93-335 DC, 21 janvier 1994, *Loi portant diverses dispositions en matière d'urbanisme et de construction*.

C. const., Décision n° 94-352 DC, 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*.

C. const., Décision n° 96-373 DC, 9 avril 1996, *Loi organique portant statut d'autonomie de la Polynésie française*.

C. const., Décision n° 96-377 DC, 16 juillet 1996, *Loi tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire*.

C. const., Décision n° 96-380 DC, 23 juillet 1996, *Loi relative à l'entreprise nationale France télécom*.

C. const., Décision n° 97-388 DC, 20 mars 1997, *Loi créant les plans d'épargne retraite*.

C. const., Décision n° 99-411 DC, 16 juin 1999, *Loi portant diverses mesures relatives à la sécurité routière et aux infractions sur les agents des exploitants de réseau de transport public de voyageurs*.

C. const., Décision n° 99-416 DC, 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*.

C. const., Décision n° 2002-461 DC, 29 août 2002, *Loi d'orientation et de programmation pour la justice*.

C. const., Décision n° 2003-467 DC, 13 mars 2003, *Loi pour la sécurité intérieure*.

C. const., Décision n° 2003-473 DC, 26 juin 2003, *Loi habilitant le Gouvernement à simplifier le droit*.

C. const., Décision n°2003-484 DC, 20 novembre 2003, *Loi relative à la maitrise de l'immigration, au séjour des étrangers en France et à la nationalité*.

C. const., Décision n° 2004-492 DC, 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*.

C. const., Décision n° 2005-527 DC, 8 décembre 2005, *Loi relative au traitement de la récidive des infractions pénales*.

C. const., Décision n° 2005-532 DC, 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

C. const., Décision n° 2007-557 DC, 15 novembre 2007, *Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile*.

C. const., Décision n°2008-562 DC, 21 février 2008, *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*.

C. const., Décision n° 2009-578 DC, 18 mars 2009, *Loi de mobilisation pour le logement et la lutte contre l'exclusion*.

C. const., Décision n° 2010-14/22 QPC, 30 juillet 2010, *M. Daniel W. et autres [Garde à vue]*.

C. const., Décision n° 2010-613 DC, 7 octobre 2010, *Loi interdisant la dissimulation du visage dans l'espace public*.

C. const., Décision n° 2010-71 QPC, 26 novembre 2010, *Mlle Danielle S*.

C. const., Décision n° 2011-625 DC, 10 mars 2011, *Loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011*.

C. const., Décision n° 2011-631 DC, 9 juin 2011, *Loi relative à l'immigration, à l'intégration et à la nationalité*.

C. const., Décision n° 2011-191/194/195/196/197 QPC, 18 novembre 2011, *Mme Élise A. et autres [Garde à vue II]*.

C. const., Décision n°2012-652 DC, 22 mars 2012 *concernant la loi relative à la protection de l'identité*.

C. const., Décision n° 2012-253 QPC, 8 juin 2012, *M. Mickaël D*.

C. const., Décision n° 2014-422 QPC, 17 octobre 2014, *Chambre syndicale des cochers chauffeurs CGT-taxis*.

C. const., Décision n° 2015-463 QPC, 9 avril 2015, *M. Kamel B et autres*.

C. const., Décision n° 2015-713 DC, 23 juillet 2015, *Loi relative au renseignement*.

C. const., Décision n° 2015-478 QPC, 24 juillet 2015, *Association French Data Network et autres*.

C. const., Décision n° 2015-722 DC, 26 novembre 2015, *Loi relative aux mesures de surveillance des communications électroniques internationales*.

C. const., Décision n° 2016-536 QPC, 19 février 2016, *Ligue des droits de l'homme*.

C. const., Décision n° 2017-637 QPC, 16 juin 2017, *Association nationale des supporters*.

C. const., Décision n° 2017-695 QPC, 29 mars 2018, *M. Rouchdi B*, *Mesures administratives de lutte contre le terrorisme*.

C. const., Décision n° 2018-765 DC, 12 juin 2018, *Loi relative à la protection des données personnelles*.

C. const., Décision n° 2019-780 DC, 4 avril 2019, *Loi visant à renforcer et garantir le maintien de l'ordre public lors des manifestations*.

C. const., Décision n° 2019-781 DC, 16 mai 2019, *Loi relative à la croissance et la transformation des entreprises*.

C. const., Décision n° 2019-810 QPC, 25 octobre 2019, *Société Air France*.

C. const., Décision n° 2020-803 DC, 9 juillet 2020, *Loi organisant la sortie de l'état d'urgence sanitaire*.

C. const., Décision n° 2020-805 DC, 7 août 2020, *Loi instaurant des mesures de sûreté à l'encontre des auteurs d'infractions terroristes à l'issue de leur peine*.

C. const., Décision n° 2021-817 DC, 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*.

C. const., Décision n° 2021-819 DC, 31 mai 2021, *Loi relative à la gestion de la sortie de crise sanitaire*.

C. const., Décision n° 2021-940 QPC, 15 octobre 2021, *Société Air France*.

C. const., Décision n° 2021-834 DC, 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*.

C. const., Décision n° 2023-850 DC, 17 mai 2023, *Loi relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions*.

B. Juridictions administratives

a. Tribunal des conflits

TC, 8 février 1873, Décision n° 00012, *Blanco*.

TC, 30 juillet 1873, Décision n° 00035, *Pelletier*.

TC, 18 décembre 1947, *Hilaire*.

TC, 7 juin 1951, Décision n° 1.316, *Dame Noualek*.

TC, 15 janvier 1968, Décision n° 01909, *Consorts Tayeb*.

TC, 5 décembre 1977, Décision n° 02060, *Demoiselle Motsch*.

TC, 12 juin 1978, *Société « Le profil »*.

b. Conseil d'État

CE, 21 juin 1895, *Cames*.

CE, sect., 6 février 1903, n° 07496, *Terrier*.

CE, 30 novembre 1906, *Jacquin*.

CE, 19 février 1909, *Abbé Olivier*, n° 27355.

CE, sect., 4 mars 1910, n° 29373, *Thérond*.

CE, 10 août 1917, n°59855, *Baldy*.

CE, ass., 17 juin 1932, n° 12045, *Ville de Castelnaudary*.

CE, 19 mai 1933, n° 17413, *Benjamin*.

CE, ass., 17 février 1950, n° 86949, *Dame Lamotte*.

CE, sect., 11 mai 1951, n° 2542, *Baud*.

CE, ass., 22 juin 1951, n° 00590 02551, *Daudignac*.

CE, sect., 23 janvier 1953, *Naud*.

CE, ass., 12 avril 1957, n° 23754, *Mimouni*.

CE, sect. 23 mai 1958, n°s 35737, 31976, 32078, *Consorts Amoudruz*.

CE, 23 octobre 1959, n° 40922, *Doublet*.

CE, 7ème et 10ème ss-sect. réunies, 10 décembre 1962, n° 55284, *Association de pêche et de pisciculture d'Orléans*.

CE, 14 décembre 1962, *Doublet*.

CE, 28 juin 1963, *Narcy*.

CE, sect., 24 mai 1968, n° 69733, *Ministère de l'Intérieur c/ Sieur Chambrin*.

CE, sect., 10 mai 1974, n° 88032, *Denoyez et Chorques*.

CE, 10 février 1982, n° 16137, *Compagnie Air-Inter*.

CE, 29 juillet 1983, n° 15116, *Baffroy-Lafitte*.

CE, 6ème et 2ème ss-sect. réunies 30 septembre 1983, n° 26611, *Fédération départementale associations agréées de pêchée l'Ain*.

CE, Sect., 9 mai 1984, n° 49153.

CE, 8 mars 1985, n° 24557, *Association les amis de la Terre*.

CE, 7ème et 10ème ss-sect. réunies, 1er avril 1994, n° 144152-144241, *Commune de Menton*.

CE, 29 décembre 1997, n° 170606, *Commune d'Ostricourt*.

CE, sect., 27 octobre 1999, n° 196306.

CE, 7ème et 5ème ss-sect. réunies, 21 juin 2000, n° 212100 et 212101, *SARL Plage « Chez Joseph »*.

CE, ord., 20 juillet 2001, n° 236196, *Commune Mandelieu-la-Napoule*.

CE, ass., 8 juillet 2005, n° 247976, *Sté Alusuisse-Lonza-France*.

CE, ord., 13 mars 2006, n° 291138, *Bayrou et Association de défense des usagers des autoroutes publiques de France*.

CE, 22 février 2007, n° 264541, *APREI*.

CE, 19 décembre 2007, n° 260327, *Sté Sogeparc*.

CE, 7ème et 2ème ss-sect. réunies, 11 mai 2009, n° 296919, *Ville de Toulouse*.

CE, 10ème et 9ème ss-sect. réunies, 16 avril 2010, n° 320196, *Association aides et autres*.

CE, 7ème et 2ème ss-sect. réunies, 3 juin 2009, n° 323594, *Société Aéroports de* Paris.

CE, 5ème et 4ème ss-sect. réunies, 10 octobre 2011, n° 337062, *Ministre de l'Alimentation, de l'Agriculture et de la Pêche*.

CE, ass., 26 octobre 2011, n° 317827, *Association pour la promotion de l'image et autre*.

CE, sect., 16 novembre 2011, n° 353172, *Ville de Paris*.

CE, 1ère et 6ème ss-sect. réunies, 4 avril 2012, n° 350952, *SNIASS*.

CE, ass., 11 avril 2012, n° 322326, *GISTI*.

CE, ord., 19 décembre 2012, n° 364444.

CE, 10ème - 9ème chambres réunies, 11 mars 2013, n° 332886, *ass. SOS Racisme*.

CE, 10ème et 9ème Sect., 9 novembre 2015, n° 376107, *Alliance générale contre le racisme et le respect de l'identité française et chrétienne*.

CE, 10ème - 9ème chambres réunies, 11 juillet 2016, n° 375977, *Ministre de l'Intérieur et ministre de la Défense*.

CE, 10ème-9ème ch. réunies, 8 février 2017, n° 393714.

CE, 10ème - 9ème ch. réunies, 18 octobre 2018, n° 404996, *Fichier TES.*

CE, 5ème et 6ème ch. réunies, 8 juillet 2019, n° 419367.

CE, 2ème - 7ème ch., 6 novembre 2019, n° 434376 et n° 434377, *Fédération des acteurs de la solidarité et autres*.

CE, ord., 18 mai 2020, n°440442.

CE, 10ème - 9ème ch. réunies, 22 décembre 2020, n°446155.

CE, ass., 21 avril 2021, n° 393099, 394922, 397844, 397851, 424717, 424718, *French data Network et a.*

CE, ord., 24 mai 2023, n° 473547, *M. B... et l'Association de défense des libertés constitutionnelles.*

c. Cours administratives d'appel

CAA Bordeaux, 2ème ch., 28 avril 1997, n° 96BX01843, *Commune d'Alès*.

CAA Marseille, 3ème ch., 26 juin 2003, n° 99MA01920, *Compagnie générale de stationnement*.

CAA Marseille, 6ème ch., 9 novembre 2009, n° 07MA00594, *Sté Vigitel*.

d. Tribunaux administratifs

TA Paris, 27 février 1963, *Société des établissements Lick et brevets Paramount*.

TA Versailles, 19 octobre 1984, *Blanchard et Monbrun*.

TA Versailles, 17 janvier 1986, *Commissaire de la République du département de Seine-et-Marne*.

TA Marseille, 9ème ch., 3 février 2020, n° 1901249.

TA Marseille, 27 février 2020, n° 1901249.

TA Paris, ord., 5 mai 2020, n°2006861/9.

TA Paris, ord., 4 novembre 2020, n° 2017540/3/5.

TA Paris, ord., 4 avril 2023, n° 2307385/9, *Association défense des libertés constitutionnelles et a.*

C. Juridictions judiciaires

a. Cour de cassation

C. cass., ch. crim., 12 juin 1952.

C. cass., ch. crim., 19 février 1957, Bull. crim. n° 165.

C. cass., ch. crim., 3 juin 1957, Bull. crim. n° 466.

C. cass., ch. crim., 17 décembre 1970, n° 68-91.412.

C. cass., ch. crim., 27 mai 1972, n° 71-91607.

C. cass., ch. crim., 24 janvier 1973, n° 72-90.691.

C. cass., ch. crim., 4 juin 1991, n° 91-81.682.

C. cass., ch. crim., 4 juin 1998, n° 96-85.871.

C. cass., ch. crim., 8 décembre 1999, n° 98-84.752.

C. cass., 27 novembre 2002, n° 02-80-659.

C. cass., ass. plén., 11 juin 2004, n° 98-82.323.

C. cass., 31 mai 2005, n° 04-85-469.

C. cass., 1ère ch. civ., 21 mars 2006, n°05-16.817.

C. cass., 1ère civ., 7 novembre 2006, n° 05-12788.

C. cass, ass. plén., 15 avril, 2011, n° 10-17.049.

C. cass., ch. crim., 3 octobre 2012, n° 11-88.468.

C. cass., ch. crim., 29 mai 2013, n° 12-85.427.

C. cass., ch. crim., 21 janvier 2014, n° 13-80.267.

C. cass., ch. soc., 18 février 2014, n° 13-10.294.

C. cass., 1ère ch. civ., 25 février 2016, n° 15-12.403.

C. cass., ch. crim., 15 novembre 2016, n° 16-85.335.

C. cass., ch. crim., 11 janvier 2017, n° 16-80.619.

C. cass., ch. crim., 3 mai 2017, n° 16-86.155.

C. cass., ch. crim., 9 janvier 2018, n° 17-82-946.

C. cass., ch. crim., 11 décembre 2018, n°18-82.365.

C. cass., ch. crim., 18 juin 2019, n°18-86-421.

C. cass., ch. crim., 8 décembre 2020, n° 20-83.885.

C. cass., ch. crim., 15 novembre 2022, n° 22-80.097.

b. Cour d'appel

CA de Paris, 7ème chambre, 15 mai 1970.

CA de Paris, 19 novembre 1986.

c. Tribunaux d'instance et de grande instance

TGI de Paris, 23 octobre 1986.

TGI de Paris, 19 mai 2006.

TGI de Bordeaux, 6 janvier 2011.

II. Décisions des ordres juridiques européens

A. Cour européenne des droits de l'Homme

CEDH, 1er juillet 1961, *Lawless c. Irlande* n° 3, n° 332/57.

CEDH, 23 juillet 1968, *Affaire relative à certains aspects du régime linguistique de l'enseignement en Belgique c. Belgique*, n° 1474/62.

CEDH, 17 janvier 1970, *Delcourt c. Belgique*, n° 2689/65.

CEDH, 18 juin 1971, *De Wilde, Ooms et Versyp c. Belgique*, n° 2832/66 et autre.

CEDH, gd. ch., 21 février 1975, *Golder c. Royaume-Uni*, n° 4451/70.

CEDH, 8 juin 1976, *Engel et autres c. Pays-Bas*, n° 5100/71 et autre.

CEDH, 7 décembre, 1976, *Handyside c. Royaume-Uni*, n° 5493/72.

CEDH, 18 janvier 1978, *Irlande c. Royaume-Uni*, n° 5310/71.

CEDH, 6 septembre 1978, *Klass c. Allemagne*, n° 5029/71.

CEDH, 26 avril 1979, *Sunday Times c. Royaume-Uni*, n° 6538/74.

CEDH, 6 novembre 1980, *Guzzardi c. Italie*, n° 7367/76.

CEDH, 2 août 1984, *Malone c. Royaume-Uni*, n° 8691/79.

CEDH, 24 mars 1988, *Olsson c. Suède* n° 1, n° 10465/83.

CEDH, 27 avril 1988, *Boyle et Rice c. Royaume-Uni*, n° 9659/82.

CEDH, gd. ch., 20 novembre 1989, *Kostovski c. Pays-Bas*, n° 11454/85.

CEDH, 19 avril 1994, *Van de Hurk c. Pays Bas*, n° 16034/90.

CEDH, 10 février 1995, *Allenet de Ribemont c. France*, n° 15175/89.

CEDH, 20 février 1996, *Vermeulen c. Belgique*, n° 19075/91.

CEDH, 25 juin 1996, *Amuur c. France*, n°19776/92.

CEDH, 19 décembre 1997, *Helle c. Finlande*, n° 20772/92.

CEDH, 27 mars 1998, *J.J c. Pays-Bas*, n° 21351/93.

CEDH, 9 juin 1998, *L.C.B. c. Royaume-Uni*, n° 14/1997/798/1001.

CEDH, 28 octobre 1998, *Osman c. Royaume-Uni*, n° 87/1997/871/1083.

CEDH 28 mars 2000, *Kiliç c. Turquie*, n° 22492/93.

CEDH, 28 mars 2000, *Mahmut Kaya c. Turquie*, n° 22535/93.

CEDH, 6 avril 2000, *Thlimennos c. Grèce*, n° 34369/97.

CEDH, 25 septembre 2001, *P.G. et J.H. c. Royaume-Uni,* n° 44787/98.

CEDH, 26 février 2002, *Fretté c. France*, n° 36515/97.

CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, n° 44647/98.

CEDH, 29 mars 2005, *Matheron c. France*, n° 57752/00.

CEDH, 20 décembre 2005, *Wisse c. France*, n° 71611/01.

CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, n° 54934/00.

CEDH, gr. ch., 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, n° 58243/00.

CEDH, gd. ch., 27 novembre 2008, *Salduz c. Turquie*, n° 36391/02.

CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04, n° 30566/04.

CEDH, 10 février 2009, *Zolotoukhine c. Russie*, n° 14939/03.

CEDH, 13 octobre 2009, *Dayanan c. Turquie*, n° 7377/03.

CEDH, 17 mars 2010, *B. B. c. France*, n° 5335/06.

CEDH, 17 mars 2010, *Gardel c. France*, n° 16428/05.

CEDH, 20 avril 2010, *Villa c. Italie*, n° 19675/06.

CEDH, 14 octobre 2010, *Brusco c. France*, n° 1466/07.

CEDH, 14 juin 2011, *Ciechońska c. Pologne*, n° 19776/04.

CEDH, 7 mars 2013, *Ostendorf c. Allemagne*, n° 15598/08.

CEDH, 18 juillet 2013, *M. K. c. France*, n° 19522/09.

CEDH, 18 septembre 2014, *Brunet c. France*, n° 21010/10.

CEDH, gr. ch., 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06.

CEDH, 30 juin 2016, *Taddeucci et McCall c. Italie*, n° 51362/09.

CEDH, 13 avril 2017, *Tagayeva et autres c. Russie*, n° 26562/07 et 6 autres.

CEDH, 22 juin 2017, *Aycaguer c. France*, n° 8806/12.

CEDH, gr. ch., 26 juin 2017, *Satakunnan markkinapörsii Oy et Satamedia Oy c. Finlande*, n° 931/13.

CEDH, 24 janvier 2019, *Catt c. Royaume-Uni*, n° 43514/15.

CEDH, 19 janvier 2021, *Lacatus c. Suisse*, n° 14065/15.

CEDH, gr. ch., 25 mai 2021, *Centrum för Rättvisa c. Suède*, n° 35252/08.

CEDH, gd ch., 25 mai 2021, *Big Brother Watch et autres c. Royaume-Uni*, n°58170/13, 62322/14 et 24960/15.

CEDH, 20 juin 2023, *Margari c/ Grèce*, n° 36705/16.

B. Cour de justice de l'Union européenne

CJCE, 29 novembre 1956, *Fédération Charbonnière de Belgique c. Haute Autorité de la Communauté européenne du charbon et de l'acier*, aff. 8/55.

CJCE, 13 juin 1958, *Compagnie des Hauts Fourneaux de Chasse c. Haute Autorité de la Communauté européenne du charbon et de l'acier*, aff. 15/57.

CJCE, 21 juin 1958, *Hauts fourneaux et aciéries belges*, aff. 8/57.

CJCE, 17 décembre 1970, *Internationale Handelgesellschaft*, aff. 11/70.

CJCE, 28 octobre 1975, *Rutili c. Ministre de l'intérieur*, aff. 36-75.

CJCE, 8 avril 1976, *Defrenne c. Belgique*, aff. C-43/75.

CJCE, 26 juin 1980, *National Panasonic c. Commission*, aff. 136/79.

CJCE, 13 novembre 1984, *Racke c. Hauptzollamt Mainz*, aff. C-283/83.

CJCE, 15 mai 1986, *Marguerite Johnston*, aff. C-222/84.

CJCE, 30 juillet 1996, *Bosphorus*, aff. C-84/95.

CJCE, 6 mars 2001, *Connolly c. Commission*, aff. C-274/99P.

CJCE, 20 mai 2003, *Österreichischer Rundfunk*, aff. jointes C-465/00, C-138/00, C-139/01.

CJCE, 12 juin 2003, *Eugen Schmidberger c. Republik Österreich*, aff. C-112/00.

CJCE, 29 janvier 2008, *Promusicae c. Telefonica de Espana*, aff. C-275/06.

CJCE, gr. ch., 3 septembre 2008, *Kadi c. Conseil de l'Union européenne et Commission des communautés européennes*, aff. jointes C-402/05 P et C-415/05 P.

CJCE, gr. ch., 16 décembre 2008, *Arcelor*, aff. C-127/07.

CJUE, gr. ch., 9 novembre 2010, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09.

CJUE, 22 décembre 2010, *DEB mbH c. Allemagne*, aff. C-279/09.

CJUE, gr. ch., 16 octobre 2012, *Commission européenne c. République d'Autriche*, aff. C-614/10.

CJUE, gr. ch., 18 juillet 2013, *Commission européenne c. Kadi*, aff. jointes C-584/10 P, C-593/10 P et C-595/10

CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland Ltd. e. a.*, aff. jointes C-293/12 et C-594/12.

CJUE, gr. ch., 6 octobre 2015, *Schrems I*, aff. C-362/14.

CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige*, aff. jointes C-203/15 et C-698/15.

CJUE, gr. ch., 26 juillet 2017, *Avis rendu en vertu de l'article 218, paragraphe 11, avis 1/15*.

CJUE, gr. ch., 16 juillet 2020, *Schrems II*, aff. C-311/18.

CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net et a.*, aff. jointes C-511/18, C-512/18 et C-520/18.

CJUE, gr. ch., 6 octobre 2020, *Privacy International*, aff. C-623/17.

CJUE, gr. ch., 22 juin 2021, *Latvijas Republikas Saelma*, aff. C-439/19.

CJUE, gr. ch., 28 septembre 2023, *La Quadrature du Net e. a. II*, aff. C-470/21.

INDEX THÉMATIQUE

Les nombres renvoient aux numéros de paragraphe

TABLE DES MATIÈRES

Sûreté et sécurité au XXIème siècle : L'exemple des drones aériens « augmentés » de sécurité publique

En 2022, le législateur a adopté un cadre autorisant le recours à des drones aériens équipés de caméras par les forces de l'ordre et les services de secours. Ces caméras aéroportées sont venues s'ajouter à l'arsenal des systèmes de vidéoprotection et s'inscrire dans le débat de la surveillance de l'espace public. De fait, les qualités mobiles et aériennes des drones aériens de sécurité publique engendrent en contrepartie une amplification des restrictions portées notamment au droit au respect de la vie privée. En outre, le traitement de données qu'ils opèrent constitue une ingérence dans le droit à la protection des données à caractère personnel. Aujourd'hui, leur possible association à des algorithmes d'analyse d'images à des fins d'aide à la prise de décisions des forces de l'ordre fait apparaître de nouveaux enjeux à l'heure où les logiciels d'Intelligence artificielle ne bénéficient pas encore d'un cadre juridique adapté. Or, cette technologie n'étant pas infaillible, les décisions prises sur le fondement des résultats de l'algorithme pourraient conduire à des arrestations voire à des détentions arbitraires. Dès lors, cette thèse entend étudier les évolutions du rapport entre la sûreté et la sécurité dans lequel s'insèrent les drones aériens « augmentés » de sécurité publique. L'étude analyse l'incidence du recours à cette technologie sur les droits et libertés, avant d'aborder le renforcement possible de leurs garanties à l'ère des technologies de surveillance « augmentées » de sécurité publique.

Personal Security and Public Safety in the 21st century : The Example of aerial drones with video analytics for public safety

In 2022, the legislature adopted a framework authorising the use of aerial drones equipped with cameras by law enforcement agencies and emergency services. These airborne cameras have been added to the arsenal of video-protection systems and become part of the debate on surveillance of public spaces. In fact, the mobile and aerial qualities of public safety drones increase the restrictions to the right to privacy. In addition, the data processing they perform constitutes an interference with the right to protection of personal data. Today, their possible association with video analytics to help law enforcement agencies make decisions is raising new issues at a time when artificial intelligence softwares do not yet benefit from an appropriate legal framework. As this technology is not infallible, decisions taken on the basis of the algorithm's results could lead to arrests or even arbitrary detention. The aim of this thesis is therefore to examine the changing relationship between personal security and public safety in the context of 'augmented' aerial drones for public safety. The study analyses the impact of the use of this technology on rights and freedoms, before looking at the possible strengthening of their guarantees in the era of 'augmented' public safety surveillance technologies.

Mots-clefs/Keywords :

Sûreté - Sécurité publique - Drones aériens - Vidéoprotection - Algorithmes d'analyse d'images - Données personnelles, Droits et libertés

Personal Security - Public Safety - Aerial Drones - CCTV - Video Analytics - Personal data - Fundamental Rights

Unité de recherche/Research unit : *Centre d'Études et de Recherches Administratives, Politiques et Sociales (CERAPS), UMR 8026, 1 place Déliot, 59000 Lille,* https://ceraps.univ-lille.fr/
Ecole doctorale/Doctoral school : *Ecole doctorale des sciences juridiques, politiques et de gestion, n° 74, 1 place Déliot, 59000 Lille, edsjpg@univ-lille.fr,* https://edsjpg.univ-lille.fr/
Université/University : *Université de Lille, 42 rue Paul Duez, 59000 Lille,* https://www.univ-lille2.fr