Université Lille Nord de France
Pôle de Recherche et d'Enseignement Supérieur

PRES Université Lille Nord de France

Thèse délivrée par

L'Université Lille 2 – Droit et Santé

Université Lille 2
Droit et Santé

N° attribué par la bibliothèque

__|__|__|__|__|__|__|__|__|__|

THÈSE

Pour obtenir le grade de Docteur en Droit

Présentée et soutenue publiquement par

ADRIEN JAMMET

Le 14/02/2018

La Prise en Compte de la Vie Privée dans l'Innovation Technologique

JURY

Directeur de thèse :

Jean-Jacques Lavenue, Professeur à l'Université Lille 2

Membres du jury:

Président	**Yves Poirmeur**, Professeur à l'Université de Versailles Saint-Quentin
Rapporteur	**Maria Belen Andreu Martinez**, Professeur à l'Université de Murcia
Rapporteur	**William Gilles**, Maître de conférences HDR à l'Université Paris 1
Examinateur	**Marcel Moritz**, Maître de conférences HDR à l'Université Lille 2

L’université n’entend donner ni approbation, ni improbation aux opinions émises dans cette thèse.

Ces opinions doivent être considérées comme propres à leur auteur.

« *La dictature parfaite serait une dictature qui aurait les apparences de la démocratie, une prison sans murs dont les prisonniers ne songeraient pas à s'évader, un système d'esclavage où, grâce à la consommation et au divertissement, les esclaves auraient l'amour de leur servitude.* »

Aldous Huxley

Remerciements

Je tiens à remercier mon directeur de thèse, Monsieur le professeur Jean-Jacques Lavenue, pour son exigence et son soutien dans la réalisation de ce travail. Les quelques qualités que le lecteur pourra trouver dans ces réflexions sont entièrement dues à ses conseils dont l'exactitude m'avait déjà frappé lors de la réalisation de mon mémoire de master 2, sous sa direction.

Je tiens également à remercier les membres de l'équipe droit du numérique du CERAPS, et particulièrement son nouveau directeur, Monsieur Marcel Mortiz, qui fut un précieux allié dans la conduite des projets dont nous avions la charge. Younes Haddadi pour son énergie et sa disponibilité. Gaylord Bauden-Hamerel pour m'avoir transmis les projets qui m'ont financé. Nora Eissa pour sa bonne humeur. Et spécialement Clémence Codron, pour sa connaissance des méandres administratifs et doctoraux.

De même, je profite de cet espace pour remercier Madame la professeur Andreu Martinez et Monsieur le professeur William Gilles pour les précieux conseils qu'ils pourront me donner en tant que rapporteurs de cette thèse, ainsi que Monsieur le professeur Yves Poirmeur, qui me fait l'honneur de présider cette soutenance.

Enfin, je remercie mes parents, ma sœur, Chrystel, Paul-Hubert, Benjamin, Thomas, Freddy, le HBCL, les Bi-licence et les jeux vidéo pour leur soutien indéfectible. Ils ne liront sans doute jamais ce travail, mais une présentation de quatre heures leur sera imposée chaque fois qu'ils s'adresseront à moi en oubliant mon titre de docteur.

Enfin, je remercie le lecteur assidu de cette thèse, qui peut me contacter sur adrien@jammet.net s'il souhaite discuter de ce travail.

Sommaire

INTRODUCTION **6**

PARTIE I

L'ADAPTATION DU DROIT AU RESPECT DE LA VIE PRIVÉE À UN PHÉNOMÈNE TECHNOLOGIQUE 32

TITRE I
L'ENCADREMENT JURIDIQUE D'UNE NOUVELLE FORME D'ATTEINTE A LA VIE PRIVEE 35

TITRE II
L'APPLICABILITE DU DROIT DANS UN CONTEXTE TECHNOLOGIQUE MOUVANT 111

PARTIE II

L'ADAPTATION DES ACTEURS DE L'INNOVATION AU RÉGIME PROTECTEUR DES DONNÉES À CARACTÈRE PERSONNEL 166

TITRE I
UNE PROTECTION LIEE AU CONSENTEMENT DE LA PERSONNE 171

TITRE II
UNE PROTECTION ERODEE PAR LE RECOURS AU CONSENTEMENT 242

CONCLUSION GÉNÉRALE **313**

BIBLIOGRAPHIE 317
INDEX 361
TABLE DES MATIERES 364
ANNEXE 369

Liste des principales abréviations

AES	*Advanced Encryption Standard*
AJDA	*L'actualité juridique - Droit administratif*
Aff.	*Affaire(s)*
Al.	*Alinéa*
AN.	*Assemblée nationale*
ANSES	*Agence Nationale de Sécurité sanitaire de l'alimentation de l'Environnement et du Travail*
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information*
API	*Application Programming Interface*
art.	*Article*
Bull.	*Bulletin de la Cour de cassation*
Bull. civ.	*Bulletin des arrêts des chambres civiles de la Cour de cassation*
Bull. crim.	*Bulletin des arrêts de la chambre criminelle de la Cour de cassation*
BVerfG	*Bundesverfassungsgericht*
c.	*Contre*
CA	*Cour d'Appel*
CAA	*Cour administrative d'appel*
Cass.	*Cour de Cassation*
Cass. Civ.	*Cour de Cassation, chambre civile*
Cass. Com.	*Cour de Cassation, chambre commerciale*
Cass. Crim.	*Cour de Cassation, chambre criminelle*
CE	*Conseil d'Etat*
CEDH	*Convention européenne des droits de l'Homme*
CESDH	*Convention Européenne de Sauvegarde des Droits de l'homme et des libertés*
CGU	*Conditions Générales d'Utilisation*
chron.	*Chronique*
CJUE	*Cour de Justice de l'Union Européenne*
CNCTR	*Commission Nationale de contrôle des techniques de renseignement*
CNIL	*Commission Nationale de l'Informatique et des Libertés*
coll.	*Collection*
COM	*Communication*
concl.	*Conclusions*
cons.	*Considérant*
CPP	*Code de procédure pénale*
DDHC	*Déclaration des droits de l'homme et du citoyen*
DGCCRF	*Direction générale de la concurrence, de la consommation et de la répression des fraudes*
dir.	*Sous la direction de*
DMP	*Dossier Médical Personnel*
éd.	*Édition*
EUROJUST	*Unité de coopération judiciaire de l'Union Européenne*
EUROPOL	*Office Européen de police*
Fasc.	*Fascicule*

FBI	*Federal Bureau of Investigation*
G29	*Groupe de travail article 29*
GAFA	*Google Apple Facebook Amazon*
Gaz. Pal.	*Gazette du Palais*
GP	*La gazette du palais*
GPS	*Global Positioning System*
HTTP	*HyperText Transfer Protocol*
IBM	*International Business Machines*
ICANN	*Internet Corporation for Assigned Names and Numbers*
INTERPOL	*International Police Organization*
iOS	*Iphone Operating System*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ISP	*Internet Service Provider*
JOAN	*Journal officiel de l'Assemblée nationale*
JOCE	*Journal officiel des Communautés Européennes*
JORF	*Journal officiel de la République Française*
JOS	*Journal officiel du Sénat*
JOUE	*Journal officiel de l'Union Européenne*
jur.	*Jurisprudence*
LPA	*Les petites affiches*
Lebon	*Recueil Lebon*
lég.	*Législation*
MAC	*Media Access Control (Adresse MAC)*
NSA	*National Security Agency*
NTIC	*Nouvelles Technologies de l'Information et de la Communication*
obs.	*Observations*
OCDE	*Organisation de coopération et de développement économique*
OMC	*Organisation mondiale du commerce*
ONDRP	*Observatoire National de la Délinquance et des Réponses Pénales*
Op. cit.	*Dans l'ouvrage cité précédemment*
p.	*Page*
PbD	*Privacy By Design*
PET	*Privacy Enhancing Technology*
PIA	*Privacy Impact Assessment*
Préc.	*Précité*
rapp.	*Rapport*
RATP	*Régie Autonome des Transports Parisiens*
Rec.	*Recueil*
Rec. Dalloz	*Recueil Dalloz*
Rééd.	*Réédition*
RFID	*Radio Frequency Identification*
RGPD	*Règlement Général sur la Protection des Données*
ROI	*Return On Investment*
RSA	*Rivest Shamir Adleman*
SAFARI	*Système informatisé pour les fichiers administratifs et le répertoire des individus*
SAP	*Systems Applications and Products for data processing*
sect.	*Section*

SMS	*Short Message Service*
SMSI	*Sommet Mondial sur la Société de l'Information*
SSID	*Service Set Identifier*
TA	*Tribunal administratif*
TES	*Fichier des Titres Electroniques Sécurisés*
TIC	*Technologie de l'information et de la communication*
TUE	*Traité sur l'Union Européenne*
UIT	*Union Internationale des Télécommunications*
v.	*Voir*
VPN.	*Virtual Private Network*
Vol.	*Volume*
W3C	*World Wide Web Consortium*
WI-FI	*Wireless Fidelity*
ZRTP	*Z Real Time Transfert Protocol*

Introduction

*

1. C'est aujourd'hui un fait, l'innovation numérique a pris une place considérable dans nos modes de socialisation[1] et dans la façon dont les Etats administrent les services régaliens[2]. Selon le ministère de l'économie, 74% de la population française utilise ces nouveaux moyens pour communiquer, dont 63% pour avoir des contacts avec les pouvoirs publics[3]. 99% des entreprises disposent d'une connexion haut débit et près de 700 000 emplois directs sont liés aux technologies de l'information et de la communication (TIC)[4]. Ce phénomène ne concerne d'ailleurs pas seulement nos modes d'interactions ou notre économie[5]. Le recours au numérique est devenu quasiment systématique, qu'il s'agisse de dispositifs de sécurité[6], de véhicules autonomes[7] ou même de santé[8].

1 À titre d'exemple, le réseau social Facebook vient récemment d'atteindre deux milliards d'utilisateurs inscrits, avec environ trente-trois millions d'utilisateurs Français actifs par mois. v. Tual Morgane, *Facebook passe la barre des deux milliards d'utilisateurs*, Le Monde, 27 juin 2017, disponible sur http://www.lemonde.fr/pixels/article/2017/06/27/facebook-passe-la-barre-des-2-milliards-d-utilisateurs_5152063_4408996.html (consulté le 01/09/17).

2 « *Si l'administration électronique est perçue dans la plupart des pays développés comme un outil de simplification pour les usagers et d'efficacité pour les administrations, dans les pays en voie de développement – et, de plus en plus, dans les pays développés -, ces technologies représentent aussi une opportunité de rationalisation du fonctionnement des administrations* ». Braun Gérard, *Rapport d'information n°402 fait au nom de la commission des Finances, du contrôle budgétaire et des comptes économiques de la Nation sur l'administration électronique au service du citoyen*, Annexe au procès-verbal de la séance du 6 juillet 2004, p. 2.

3 Ministère de l'économie et des finances, *Chiffres clés du numérique*, édition 2016.

4 Ibid.

5 v. Babinet Gilles, *L'Ere Numérique, Un Nouvel âge de l'Humanité : Cinq Mutations Qui Vont Bouleverser Notre Vie*, Le Passeur éditeur, janvier 2014, 236 p.

6 « *Pour l'autorité publique, l'objectif de ces techniques est double : sécuriser l'authentification et l'identification des personnes, d'une part, et rendre l'action administrative plus efficace, d'autre part* ». Bonhomme François, Leconte Jean-Yves, *Rapport d'information n°788 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'usage de la biométrie en France et en Europe*, Enregistré à la Présidence du Sénat le 13 juillet 2016, p. 8.

7 v. Chatellier Régis, *Le véhicule connecté, porteur d'enjeux autour des données*, Laboratoire d'Innovation Numérique de la CNIL, 7 juin 2016.

8 McGoogan Cara, *NHS illegally handed Google firm 1.6m patient record, UK Data watchdog finds*, The Telegraph, 3 July 2017.

2. Cela représente un changement de paradigme important dans la façon dont les Etats et les entités privées envisagent ce que le manuel d'Oslo de l'Organisation de Coopération et de Développement Economique (OCDE) nomme : « *l'innovation technologique de produit et de procédé »*[9]. En effet, si certains peuvent considérer les prouesses du numérique comme une révolution[10], il demeure que ses apports se définissent avant tout comme deux composants de l'innovation technologique, soit en tant que produit technologiquement nouveau[11], soit comme une amélioration technologique d'un produit déjà existant[12]. Mais dans ce contexte, faire reposer l'innovation technologique sur un même facteur de croissance crée une dépendance qui génère une fragilité structurelle. L'ensemble de cet écosystème numérique, dans lequel puise l'innovation technologique, repose un même socle juridique issu du régime protecteur de la vie privée, celui encadrant les possibilités de traitement des données à caractère personnel. De ses qualités et de ses défauts dépendra la pérennité de l'innovation technologique, mais également l'efficacité de la protection de la vie privée des citoyens face à celle-ci.

3. Pour cette raison, la question de l'évolution du droit au respect de la vie privée face à l'innovation technologique apparait comme l'une des problématiques juridiques prééminentes de ce début du XXIème siècle.

9 « *Les innovations technologiques de produits et de procédé (TPP) couvrent les produits et procédés technologiquement nouveaux ainsi que les améliorations technologiques importantes de produits et de procédés qui ont été accomplis* ». Organisation de Coopération et de Développement Economiques, *Manuel d'Oslo*, *Principes directeurs pour le recueil et l'interprétation des données sur l'innovation*, 3eme édition, 2005, p. 36.

10 v. Roques-bonnet Marie-Charlotte, *Le Droit Peut-il Ignorer La Révolution Numérique ?*, Michalon, 4 novembre 2010, 606 p. ; Bravo Alain, *La Société et l'Economie à l'Aune de la Révolution Numérique : Enjeux et Perspectives des Prochaines Décennies*, La Documentation Française, 29 octobre 2009, 102 p.

11 « *Un produit technologiquement nouveau est un produit dont les caractéristiques technologiques ou les utilisations prévues présentent des différences significatives par rapport à ceux produits antérieurement. De telles innovations peuvent faire intervenir des technologies radicalement nouvelles, ou reposer sur l'association de technologies existantes dans de nouvelles applications, ou découler de la mise à profit de nouvelles connaissances* ». Organisation de Coopération et de Développement Economiques, *Manuel d'Oslo*, *Principes directeurs pour le recueil et l'interprétation des données sur l'innovation*, 3eme édition, 2005, p. 37.

12 « *Un produit technologiquement amélioré est un produit existant dont les performances sont sensiblement augmentées ou améliorées. Un produit simple peut être amélioré (par amélioration des performances ou abaissement du coût) grâce à l'utilisation de composants ou de matériaux plus performants, ou bien un produit complexe, qui comprend plusieurs sous-systèmes techniques intégrés, peut être amélioré au moyen de modifications partielles apportées à l'un des sous-systèmes* ». Ibid, p. 37.

4. Principe constitutionnel longtemps associé à la liberté individuelle[13], la protection de la vie privée a mué avec le temps pour prendre en compte les différents aspects de la vie sociétale[14], soulignant ainsi son rôle décisif dans nos modèles juridiques, politiques et sociaux[15]. Pourtant, bien que la notion de vie privée soit essentielle à l'ordre juridique, celle-ci ne fit jamais l'objet d'une définition générale par le législateur ou les juges. Pour la Cour Européenne des droits de l'Homme, il n'est « *ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de ''vie privée''* »[16]. Il serait même restrictif de *« la limiter à un cercle intime où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables* »[17].

13 v. Conseil Constitutionnel, Décision n°76-75 du 12 janvier 1977, *Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales* ; Conseil Constitutionnel, Décision N° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 - Journal officiel du 21 janvier 1995, p. 1154 ; Conseil Constitutionnel, Décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universell*e, Rec. p. 100 - Journal officiel du 28 juillet 1999, p. 11250, considérant 45.

14 Selon la Commission Nationale de l'Informatique et des Libertés: « *C'est indéniable, la protection des données n'a jamais été autant sur le devant de la scène qu'en 2016, et la CNIL est de plus en plus sollicitée, qu'il s'agisse des pouvoirs publics, des professionnels ou des particuliers* ». v. Commission Nationale de l'Informatique et des Libertés, *Rapport d'activité 2016*, La Documentation Française, p10. Du côté des particuliers, cela s'explique par une utilisation croissante des services numériques, créant un phénomène de numérisation des échanges privés. Pour Caroline Vallet : « *Le développement des sites de réseau social a engendré des changements significatifs. En effet, le fait de dévoiler sa vie privée sur un média à vocation publique représente un nouveau comportement que l'on ne rencontrait jusqu'alors que chez les personnalités publiques ou les célébrités. Désormais, chacun de nous peut devenir une personne publique et se créer une certaine notoriété, même si elle peut ne se limiter qu'à Internet* ». Vallet Caroline, *Le Dévoilement de la Vie Privée sur les Sites de Réseau Social, des Changements Significatifs*, Droit et Société n°80, 2012/1, p. 163. Du côté des pouvoirs publiques, on peut rappeler l'importance croissante des techniques numériques pour l'administration, soulignée dès 2004 par le Sénateur Gérard Braun : « *D'une façon générale, les choix technologiques des Etats ont un impact déterminant sur les liens que les citoyens établissent avec leurs administrations, et sur l'efficience de ces dernières* ». v. Braun Gérard, *Rapport d'information n°402 fait au nom de la commission des finances, du contrôle budgétaire et des comptes économiques de la Nation sur l'administration électronique au service du citoyen*, Annexe au procès-verbal de la séance du 6 juillet 2004, p5.

15 Pour une étude de l'importance du rôle de la vie privée dans les modèles juridiques, politiques et sociaux, on peut citer succinctement : Arendt Hannah *Responsabilité et Jugement*, Payot, 5 mars 2009, 362 p. ; Schopenhauer Arthur, *Essai sur le Libre Arbitre*, Rivages, 2 mars 1992, 176 p. ; Mill John Stuart, *De la Liberté*, Jean-Marie Tremblay, 19 mai 2002, p. 13.; ou bien dans le domaine juridique : Ochoa Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Droit. Université Paris 1 Panthéon-Sorbonne, 2014, HAL Id : Tel-01340600 ; Roussillon Henry, *Liberté Personnelle: une Autre Conception de la Liberté ?*, Presses de l'Université des Sciences Sociales de Toulouse, 1 juin 2006, 159 p. ; Bioy Xavier. *Le Libre Développement de la Personnalité en Droit Constitutionnel Essai de Comparaison (Allemagne, Espagne, France, Italie, Suisse),* Revue internationale de droit comparé. Vol. 55 N°1. Janvier-mars 2003, pp. 123-147.

16 CEDH, 16 décembre 1992, *Niemietz c. Allemagne*, n°13710/88, considérant 29.

17 Ibid.

5. Pour pallier cette difficulté, la Cour reprend la définition de l'article 8 de la Convention Européenne des droits de l'homme et des libertés fondamentales qui stipule que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* »[18], sans qu'une hiérarchie ne soit imposée entre ces éléments juxtaposés. Les autres textes internationaux régissant cette notion utilisent d'ailleurs la même formulation, qu'il s'agisse de la Déclaration universelle des droits de l'homme de 1948[19], du Pacte international relatif aux droits civils et politiques de 1966[20] ou de la Charte des droits fondamentaux de l'Union Européenne de 2000[21]. Par conséquent, si l'on peut trouver dans la jurisprudence de la Cour Européenne des éléments identifiés relevant de la vie privée, tel que la liberté de choisir son lieu de domiciliation[22] ou l'orientation sexuelle[23], il n'existe pas de méthodologie ou de définition qui circonscrivent la notion. Cette absence entraine une véritable difficulté lorsqu'il s'agit de qualifier un nouvel élément.

6. Sur ce point, le droit interne n'est d'aucun secours. Le Code Civil ne fait qu'énoncer le droit au respect de la vie privée sans le définir[24] et le Code Pénal contourne la problématique en ciblant seulement ses atteintes, punissant par ses articles 226-1 et suivants le fait de porter atteinte à son intimité en captant, enregistrant ou transmettant sans consentement des paroles, ainsi qu'en fixant, enregistrant ou transmettant sans consentement l'image d'une personne[25].

---

18 Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4,XI, 1950, article 8.

19 Déclaration Universelle des Droits de l'Homme, texte adopté le 10 décembre 1948 par l'assemblée générale des Nations Unies, article 12.

20 Pacte international relatif aux droits civils et politique, Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale des Nations Unis dans sa résolution 2200 A (XXI) du 16 décembre 1966, article 17.

21 Charte des Droits Fondamentaux de l'Union Européenne, 2000/C 364/01, Journal Officiel des Communautés Européennes, 18 décembre 2000, article 7.

22 CEDH, 25 septembre 1996, *Buckley c. Royaume-Uni*, n°20348/92. « La Cour a souvent souligné que l'expression de « vie privée » est large et ne se prête pas à une définition exhaustive. Des éléments tels que le sexe, l'orientation sexuelle et la vie sexuelle sont des composantes importantes du domaine personnel protégé par l'article 8 ». CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, n° 42758/98 et 45558/99.

23 « *La Cour a souvent souligné que l'expression de « vie privée » est large et ne se prête pas à une définition exhaustive. Des éléments tels que le sexe, l'orientation sexuelle et la vie sexuelle sont des composantes importantes du domaine personnel protégé par l'article 8* ». CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, n° 42758/98 et 45558/99.

24 Code Civil, article 9 : « *Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, 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* ».

25 Code Pénal, article 226-1 : « *Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre*

7. À l'étranger, aucune liste figée du contenu de la vie privée n'a été fixée. La Cour Constitutionnelle d'Afrique du Sud la définit comme « *le droit d'une personne à vivre sa vie comme elle l'entend* »[26], tandis que la Cour Suprême du Canada la considère comme une protection de la « *sphère limitée d'autonomie personnelle dans laquelle les individus peuvent prendre des décisions intrinsèquement privées sans intervention de l'Etat* »[27].

8. La doctrine s'est logiquement employée à combler ce vide. D'abord en tant que concept d'indépendance de la personne vis-à-vis de son entourage, à l'instar de Samuel Warren et Louis Brandeis qui le définissent comme le « *droit d'être laissé seul* » [28]. Puis en proposant une définition de la vie privée en opposition avec ce qui relève de la vie publique, aidée par une approche au cas par cas éliminant de son contenu l'ensemble des éléments extérieurs à son essence, tels que les activités réalisées à l'extérieur du domicile[29]. Contextualisé ainsi, le droit au respect de la vie privée semble devenir une sorte de droit résiduel, voué uniquement à protéger les activités exclusivement privées.

9. À l'opposé de ces tentatives de définitions par la négative, Daniel Gutmann a avancé l'idée de considérer la vie privée comme une somme positive : celle de l'ensemble des informations personnelles d'un individu, au sens de « *l'information qui entretient avec le sujet un lien si étroit qu'elle permet à celui qui la possède d'acquérir une connaissance approfondie de la personne concernée* » [30]. Cependant, cette dernière proposition semble laisser de côté les aspects sociaux de la vie privée, alors même que pour Yves Poullet et Antoinette Rouvroy, ceux-ci sont le centre du concept. Selon ces derniers: « *le droit à la protection de la vie privée, nonobstant le fétichisme dont il est l'objet à la fois pour nombre de ses défenseurs les plus acharnés, et pour ses détracteurs les plus irréductibles, n'est rien*

---

privé ou confidentiel ; 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé ».

26 Constitutional Court of South Africa, NM and Others v. Smith and Others (Freedom of Expression Institute as Amicus Curia), 2007, 5, SA 250 (CC), Case CCT 69/05, point 33: « *Privacy encompasses the right of a person to live his or her life as he or she pleas*e ».

27 Jugement de la Cour Suprême, 31 octobre 1997, Goodbout c. Longueuil (Ville), 1997, R.C.S, 844.

28 « *Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, -- the right to be let alone* ». Warren Samuel, Brandeis Louis, *The Right to Privacy*, Harvard Law Review, vol. IV, December 15, 1890, p. 193.

29 v. en ce sens : Lindon Raymond, *La Presse et la Vie Privée*, JCP, 1975, I, 1887.

30 Gutmann Daniel*, Le sentiment d'identité,* L.G.D.J., p. 226.

d'autre qu'un instrument au service des capacités de développement personnel autonome, qui sont, dans une société donnée et à une époque donnée, nécessaire au fonctionnement démocratique du régime politique en vigueur »[31].

10. Ces réflexions ne furent jamais reconnues unanimement par la jurisprudence, qui restera cantonnée à une application sélective du droit au respect de la vie privée, identifiant progressivement ses éléments intrinsèques avec chaque cas d'espèce. Cette approche a d'ailleurs un sens. Si l'absence de fixité conceptuelle rend difficile la prévisibilité de l'appréciation des juges face à un élément qui n'aurait pas préalablement été reconnu, elle permet d'éviter de circonscrire une notion dont la définition, éminemment circonstancielle, reflète la manière dont chacun conçoit sa propre existence. Ainsi, pour Lucien Martin : « *il parait impossible, d'un mot, d'une formule, de dire à l'avance où finit la vie privée, où commence la vie publique. Il semble bien que cette question sera toujours dans la dépendance de l'appréciation souveraine des tribunaux* »[32].

11. Mais si une telle conception était viable dans le monde précédant l'informatique, le morcèlement du droit au respect de la vie privée trouve sa limite dans la société de l'information[33]. Les progrès concernant les facilités de partage de données ont graduellement rendu illusoire l'idée doctrinale[34] ou jurisprudentielle d'une « *sphère d'intimité de la vie privée* »[35] contrôlée par l'individu. Les utilisateurs partagent en ligne des informations dont s'emparent des dizaines d'entités privées afin de les valoriser[36], et les Etats utilisent de plus en

31 Poullet Yves, Rouvroy Antoinette, *Le Droit à l'Autodétermination Informationnelle et la valeur du développement personnel. Une Réévaluation de l'importance de la vie privée pour la démocratie*, Etat de Droit et virtualité, Ed. Karim Benyekhlef & Pierre Trudel, Montréal: thémis, 2009, p. 161.

32 v. Martin Lucien, *Le Secret de la Vie Privée*, Sirey, 1959, 256 p. Pour une définition du concept de société de l'information, v. Neveu Erik, *Une Société de Communication ?,* Montchrestien, 15 juin 2011, 160 p. ; Curien Nicolas, Muet Pierre-Alain, *La Société de l'Information*, La documentation Française, 2004, 312 p. ; Castells Manuel, *La Société en Réseaux*, Fayard, 21 février 2001, 674 p.

33 Pour une définition du concept de société de l'information, v Neveu Erik, *Une Société de Communication ?,* Montchrestien, 15 juin 2011, 160 p. ; Curien Nicolas, Muet Pierre-Alain, *La Société de l'Information*, La documentation Française, 2004, 312 p. ; Castells Manuel, *La Société en Réseaux*, Fayard, 21 février 2001, 674 p.

34 Idée partagée par de nombreux auteurs, dont les plus éminents sont sans doute Jean Carbonnier et Gérard Cornu, selon lesquels il existerait une sphère d'intimité dont l'individu peut exclure les tiers. v. Carbonnier Jean, *Droit Civil*, vol. 1, PUF, 8 octobre 2004, p. 425 ; Cornu Gérard, *Vocabulaire Juridique,* PUF, 13 janvier 2016, 1152 p.

35 Notion que l'on retrouve largement dans la jurisprudence. A titre d'exemple, v. TGI. Paris, 22 avril 1992. ; TGI Paris 15 décembre 1993 ; TGI. Nanterre, Section C, 27 octobre 1998.

36 v. index : Data Broker.

plus les technologies numériques pour faciliter le travail de leurs administrations[37]. Dans ce nouvel environnement, définir le périmètre de la sphère de la vie privée devient une question dépassant le cadre juridique, faute d'un élément concret auquel se rattacher.

12. Dès lors, lorsqu'il fut confronté aux premières affaires soulignant les craintes de la population face à l'usage régalien de l'informatique[38], le législateur prit l'option de désigner la donnée à caractère personnel comme pivot central d'un nouveau dispositif de protection spécifique, sans s'enchainer à celui déjà existant relatif à la protection de la vie privée. Selon Jean Foyer, s'exprimant devant l'Assemblée Nationale en 1977 : « *il convient, dans une matière aussi neuve, de se souvenir du proverbe : Qui trop embrasse mal étreint. C'est pourquoi le projet prévoit que les dispositions légales s'appliqueront seulement aux traitements automatisés d'informations nominatives, les seules qui soient vraiment dangereuses pour la vie privée et pour les droits individuels des citoyens, et distingue selon que le traitement sera mis en œuvre par une personne morale de droit public ou une personne morale gérant un service public — cela vise les organismes de sécurité sociale — d'une part, ou par une personne physique ou morale privée, d'autre part* »[39].

13. Ces réflexions donnèrent naissance à la loi informatique et libertés du 6 janvier 1978[40] et la donnée à caractère personnel devint une représentation matérielle de ce qu'est le droit au respect de la vie privée transposé dans le monde numérique, définie comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »[41]. Restée quasiment intacte jusqu'à aujourd'hui avec le récent règlement général sur la protection des données[42], cette définition s'applique de

37 v. Ministère de l'économie et des finances, *Chiffres clés du numérique*, édition 2016.
38 Boucher Philippe, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.
39 Foyer Jean, *Déclaration devant l'Assemblée Nationale*, Séance du mardi 4 octobre 1977, JO n°79 du 5 octobre 1977, pp. 134-150.
40 Loi n° 78-17 du 6 janvier 1978, *Op. Cit.*
41 Ibid, article 2.
42 « *«données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;* ». 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*

manière transversale à l'ensemble des traitements de données, dans un régime général fondé essentiellement sur le consentement de l'utilisateur. Seules certaines catégories de données échappent aux dispositions générales, à l'instar des données sensibles[43] nécessitant l'obtention préalable d'une autorisation de la Commission Nationale de l'Informatique et des Libertés (CNIL) avant tout traitement[44].

14. Mais en devenant l'élément fondateur de la protection, la donnée à caractère personnel a, semble-t-il, remplacé le concept de vie privée dans le numérique. En cas de litige relatif au numérique, il ne s'agira plus de savoir si la vie privée est atteinte, mais si les données personnelles ont été traitées de manière compatible avec le régime qu'on leur a attribué. Or, la différence de périmètre de protection, entre une absence opportune de définition du droit au respect de la vie privée et une circonscription de celui-ci à un élément figé dans le numérique engendre nécessairement un questionnement sur la pertinence du régime protecteur des données à caractère personnel et sur sa capacité à protéger la vie privée à l'ère numérique.

15. Le terrain d'étude que constitue la prise en compte de la vie privée dans l'innovation technologique offre une parfaite représentation de ce nouveau paradigme. L'intégration de la vie privée dans l'innovation est un exemple concret de la traduction du droit au respect de la vie privée dans le monde numérique, et l'observation de l'utilisation du régime applicable aux données à caractère personnel par les grands acteurs informatiques et les Etats permet d'en apprécier la solidité. Conjointement, ces deux aspects souligneront l'intérêt de l'objet principal de notre étude.

---

directive 95/46/CE, Règlement général sur la protection des données, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

43 Les données sensibles sont celles mentionnées à l'article 8-I de la loi informatique et libertés qui dispose : « *Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». Loi informatique et libertés du 6 janvier 1978, Op. Cit, article 8.

44 Selon l'article 25 de la loi informatique et libertés : « *Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8* ». Loi informatique et libertés du 6 janvier 1978, Op. Cit. Article 25. Pour un exemple d'autorisation unique, v. Commission Nationale de l'Informatique et des Libertés, Délibération n°2010-336 du 22 juillet 2010 *autorisant la mise en œuvre par la société Morpho d'un traitement de données à caractère personnel ayant pour finalité principale la recherche sur les algorithmes biométriques,* Publiée sur Légifrance le 14 octobre 2015 ; Commission Nationale de l'Informatique et des Libertés, Délibération n°2017-013 du 19 janvier 2017 *autorisant l'Assistance Publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé EDS*, Publiée sur Légifrance le 4 mars 2017.

Objet de l'étude

16. L'étude de la prise en compte de la vie privée dans l'innovation technologique est celle du régime juridique applicable aux données à caractère personnel. Cependant, la complexité contextuelle du sujet impose une analyse pragmatique, intégrant les éléments économiques et technologiques pour définir l'utilisation effective du droit dans et par l'innovation numérique. Cela passe nécessairement par une approche phénoménologique, rappel historique sur le cheminement juridique qui a conduit le législateur à choisir une telle forme de protection, passant d'un droit au respect de la vie privée général à un régime spécifique applicable aux données à caractère personnel, puis à une observation de son efficacité à protéger l'essence de la vie privée.

17. Au cœur de ce travail se trouve la volonté d'apporter des éléments de réponse objectifs permettant d'expliquer l'écart existant entre la confiance que les Français accordent à la technologie pour respecter leur vie privée, et les déclarations des législateurs Européens et Français sur l'efficacité des textes protecteurs. En effet, selon certains sondages, 74% des personnes interrogées ne faisaient pas confiance aux applications mobiles quant à l'utilisation de leurs données[45]. De même, si 84% des personnes pensent que les plateformes sociales utilisent leurs données pour leur adresser des messages publicitaires personnalisés, 81% sont gênés par cette pratique[46].

18. Ainsi, si l'on devait résumer l'objet de notre étude à un questionnement, ce serait celui de l'efficacité réelle du régime de protection de la vie privée dans l'innovation technologique. Dans un tel contexte, les utilisateurs ont-ils raison d'être méfiants vis-à-vis de l'innovation numérique quant à son respect de leur vie privée ?

---

45 Selon le barometre Odoxa-Microsoft-L'Usine. v. Eustache Sophie, *Données personnelles : ¾ des Français ne font pas confiance aux applis mobiles*, L'Usine Digitale, 21 avril 2016, disponible sur http://www.usine-digitale.fr/article/donnees-personnelles-3-4-des-francais-ne-font-pas-confiance-aux-applis-mobiles.N387806 (consulté le 01/09/17).

46 Puiatti Sonia, *Seulement 37% des Français sont confiants dans l'usage d'Internet*, EcommerceMag, 24 octobre 2016, disponible sur http://www.ecommercemag.fr/Thematique/indicateurs-1010/Breves/Seulement-Fran-ais-sont-confiants-dans-usage-Internet-309918.htm (consulté le 01/09/17).

Contexte de l'étude

19. Afin de mesurer la prise en compte de la vie privée dans l'innovation technologique, nous devons nécessairement nous placer face au nouveau paradigme que constitue celle-ci pour le droit au respect de la vie privée.

20. Pour cela, il faut commencer par reconnaître l'évolution de la fonction du droit au respect de la vie privée, ou du moins l'évolution de la manière dont le législateur la conçoit pour le numérique. Selon les nombreuses déclarations[47] entourant la conception puis la publication du règlement général sur la protection des données[48], il ne s'agit plus seulement de considérer la protection de la personne humaine comme un objectif unique, mais d'y adjoindre les aspects économiques dépendants de la faculté de commercialiser les données[49].

21. Selon Neelie Kroes, commissaire Européenne à la société numérique qui s'exprimait en 2013 lors de la phase de négociation du règlement général sur la protection des données : « *dans un moment où l'Europe a désespérément besoin de croissance, ceci [l'innovation*

47 v. Reeding Viviane, Déclaration *publique: The EU Data Protection Reform 2012 : Making Europe The Standard Setter For Modern Data Protection Rules In the Digital Age lors de l'Innovation Conference Digital, Life, Design*, Munich, 22 January 2012 ; European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*, COM(2012), 11, Final, 25 January 2012, Brussels ; Groupe de Travail « Article 29 » sur la protection des données, *Opinion 08/2012 providing further input on the data protection reform discussions*, Adopted on 5 October 2012, 01574/12/EN, WP 199. ; Commission Nationale de l'Informatique et des libertés, *Règlement Européen : ce qui change pour les professionnel, Communication du 15 juin 2016*, disponible sur https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels (consulté le 01/09/17) ; Commission Nationale de l'Informatique et des Libertés, *Consultation publique sur le règlement Européen, Synthèse des contributions sur la notification de violations, le consentement, le profilage*, Communication datée de mars 2017.

48 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

49 « *This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities* ». European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*, COM(2012), 11, Final, 25 January 2012, Brussels, p2.

technologique] est exactement vers où nous devrions nous tourner pour créer de nouveaux emplois et de nouvelles opportunités. C'est pour cela que j'ai défini les données comme le nouveau pétrole. Parce que c'est un carburant pour l'innovation, faisant fonctionner notre économie » [50]. Par conséquent : « *cette révolution numérique, orientée vers l'économie de la donnée, a besoin d'une aide et d'un cadre législatif adapté. Les données doivent être accessibles librement et pouvoir être réutilisées. Cela nécessite des facilités de transports et d'interopérabilités, sans différence de règles ou de standards pour chaque pays ou type de données. Cela requiert également un cadre juridique protecteur de la vie privée construisant la confiance* »[51]. Ce nouveau cadre, incarné par le règlement général sur la protection des données[52], est donc à la recherche d'un équilibre entre les deux aspects, à priori antagonistes, que sont une protection renforcée et un partage maximal des données.

22. Cette vision pragmatique s'explique par le potentiel de l'innovation numérique pour le marché Européen. Selon la Commission Européenne : « *le marché unique numérique a pour objectif de faire tomber les obstacles d'ordre réglementaire et de faire enfin de 28 marchés nationaux un seul marché unique. Un marché unique numérique totalement opérationnel pourrait représenter une contribution de 415 milliards d'euros par an pour notre économie et créer des centaines de milliers de nouveaux emplois* »[53]. Mais cela va plus loin qu'une simple opportunité pour les entreprises. Selon une étude du cabinet McKinsey, 300 milliards de dollars pourraient être générés chaque année par le système de santé Américain et 250 milliards pour le secteur publique Européen[54].

23. L'engouement pour cette manne économique se traduit par une activité législative particulièrement intense. Au niveau Français avec la réforme de la loi informatique et libertés

50 Traduction par l'auteur de « *At a time when Europe desperately needs growth, this is exactly where we should be looking to create new jobs and new opportunities.That's why I've called data the new oil. Because it's a fuel for innovation, powering and energising our economy* ». Kroes Neelie, *Declaration publique à occasion de l'EIT Foundation Annual Innovation Forum: The Big Data Revolution*, Bruxelles, 26 mars 2013.

51 Traduction par l'auteur de « *But this data revolution, moving to a data-driven economy, won't happen by itself. It needs a helping hand, and the right framework. Data needs to be freely available for use and re-use. It needs to be easy to transport and inter-operate — without different rules and standards for every country and dataset. And it needs the framework that safeguards privacy and builds trust.* ». Ibid.

52 Règlement général sur la protection des données, 4 mai 2016, Op. Cit.

53 Commission Européenne, *Un marché unique numérique pour l'Europe : la Commission définit 16 initiatives pour en faire une réalité*, IP 15/4919, Bruxelles, 6 mai 2015.

54 McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity*, May 2011, p. 3.

par la loi du 7 octobre 2016 pour une République numérique[55]. Et au niveau Européen avec l'adoption du règlement général sur la protection des données[56] ayant abrogé la directive 95/46/CE[57], ainsi que la proposition de règlement vie privée et communication électronique abrogeant la directive 2002/58/CE[58] qui fut publiée le 10 janvier 2017[59]. L'ensemble de ces textes repose sur une idée commune : faire de l'individu l'acteur de sa propre protection[60]. Cette idée « *d'empowerment* »[61] s'oppose à celle d'un contrôle rigoureux des transferts de données par la voie législative, laissant la personne concernée décider seule de l'usage qui peut être fait de ses données.

24. Néanmoins, face à cette nouvelle conceptualisation du régime de protection, certains avancent l'idée que la ruée vers l'or numérique se fait au détriment de la protection de la vie privée. La Quadrature du net fustige le *« jeu de dupe que constitue le principe « gratuité contre données personnelles », qui tend à devenir le modèle dominant* »[62]. En effet, à la faveur du régime applicable aux données à caractère personnel, de nombreux sites internet ont mis en place des règles de confidentialité[63], auxquels l'usager doit souscrire obligatoirement, rendant licite un périmètre d'exploitation particulièrement vaste des données. Cela entraine un phénomène de contractualisation des relations entre personnes concernées et services

55 Loi n°2016-1332 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016, texte n°1.

56 Règlement général sur la protection des données, 4 mai 2016, Op. Cit.

57 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

58 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

59 Commission Européenne, *Proposition de règlement du Parlement Européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement vie privée et communication électronique),* 10 janvier 2017, Bruxelles, COM(2017) 10 final.

60 « *Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant* », Règlement général sur la protection des données, 4 mai 2016, considérant 7, Op. Cit.

61 « *The potential for new value creation from allowing data to flow and combine with other data needs to be balanced against the potential risks and intrusions this could cause. This requires a shift in thinking from focusing on data protection to enabling data empowerment* ». World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, Prepared in collaboration with the Boston Consulting Group, February 2013, p. 12.

62 La Quadrature du Net, *Données personnelles et vie privée : la Quadrature du net répond à la Commission européenne*, Paris, 22 juin 2016.

63 On peut citer à titre d'exemple Google, ayant récemment fusionné l'ensemble des règles de confidentialité de ses différents services en un seul texte, applicable uniformément, amenant la CNIL à se pencher sur la licéité d'une telle procédure. v. Commission Nationale de l'Informatique et des Libertés, *Lettre adressée à Google Inc,* Paris, 27 février 2012.

numériques, dans lequel le responsable de traitement devient le principal acteur grâce à sa maitrise des règles qui vont fixer cette relation. Cette libéralisation entraine un partage étendu des données, dont les data brokers[64] sont les premiers bénéficiaires. À titre d'exemple, Experian[65], l'un des leaders du marché, vend un fichier appelé Mosaic contenant 95% des foyers Français, classés selon leur nombre de membres, leur revenu, leur localisation et leur comportement[66].

25. Or, pour Nicola Ochoa, « *bien qu'il soit [le consentement] largement consacré en droit, les textes restent relativement muets sur sa signification. Or celle-ci est assez éloignée d'une vision naïve selon laquelle il ne s'agirait que de redonner à la personne fichée la « maitrise de ses données ». Bien au contraire, elle s'inscrit dans une dynamique de simplification de la réglementation relative aux traitements de ce type de données, autant pas ses effets que par ses exceptions* » [67]. Selon ces réflexions, le consentement ne deviendrait dès lors qu'un moyen pour les plateformes de services informatiques d'abuser de leurs utilisateurs, en échangeant l'accès à celles-ci contre une collecte particulièrement vaste de leurs données. Par conséquent, en réduisant la protection au seul consentement, le législateur aurait détourné la liberté de consentir au profit des intérêts économiques en présence. On pourrait donc résumer ce débat à la célèbre citation de Lacordaire : « *entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime, et la loi qui affranchit* » [68]. Tout dépend, dans ce contexte, de la véracité que l'on peut accorder à celle-ci lorsqu'il s'agit d'étudier le régime de protection des données.

64 « *Le terme de data broker ou courtier de données désigne une entreprise dont l'activité est basée sur la revente de données à des annonceurs ou à des prestataires marketing. Dans le contexte marketing, les données vendues par les data brokers peuvent être utilisées pour le ciblage de campagne marketing, pour de la professionnalisation / recommandation dynamique sur les sites et applications mobiles ou à des fins d'études. Au sens strict du terme, un data broker ne collecte pas directement la donnée consommateur. Il se « contente » de l'acheter pour la revendre ensuite aux acteurs intéressés avec un processus de traitement / valorisation* ». Bathelot Bertrand, *Définition: Data Broker*, Définition Marketing, Encyclopédie illustrée du marketing, 22 mars 2017, disponible sur https://www.definitions-marketing.com/definition/data-broker/ (consulté le 01/09/17).

65 v. www.experian.fr, (consulté le 01/09/17).

66 Dasquié Guillaume, *Le Business Secret des Data-Brokers*, GQ, 25 janvier 2016, disponible sur http://www.gqmagazine.fr/pop-culture/gq-enquete/articles/le-business-secret-des-data-brokers/29845 (consulté le 01/09/17).

67 Ochoa Nicolas, *Pour en Finir avec l'Idée d'un Droit de Propriété sur ses Données Personnelles : Ce que Cache Véritablement le Principe de Libre Disposition*, RFDA, 2015, n°6, pp. 1157.

68 Lacordaire Henri*, Conférences de Notre-Dame de Paris*, Sagnier et Bray, 1848, p. 246.

26. Par conséquent, il conviendra de placer notre étude dans son environnement concret, sans considérer le choix du législateur comme dénué d'idéologie ou de portée vis-à-vis du droit au respect de la vie privée.

27. Pour autant, il serait préjudiciable d'évaluer la pertinence de la législation sous le regard unique de son implication économique. Celle-ci cherche également à refléter une véritable évolution technologique avec l'apparition du *Big Data*[69], ainsi qu'à pérenniser l'innovation dans ce domaine. Ce nouveau concept, dont aucune définition précise n'emporte de consensus[70], semble indiquer que les outils numériques sont aujourd'hui capables de produire et de traiter une masse considérable de données en améliorant l'efficacité des services actuels. Dans le cadre des *smart cities*[71] par exemple, il est possible d'imaginer des systèmes de circulation des transports en commun en fonction de l'activité humaine détectée en direct dans les stations de métro[72]. On trouve également des applications dans des domaines aussi variés que la santé[73], la science[74] ou l'écologie[75]. En cela, le *big data* représente des enjeux importants en termes d'innovation, pouvant servir les citoyens

69 « *Au départ, le concept a indiqué qu'à cause d'un volume d'informations devenu énorme, les capacités-mémoire des ordinateurs pour effectuer leur traitement étaient dépassées, et les ingénieurs devaient modifier les outils utilisés pour les analyser dans leur totalité. C'est là l'origine de nouvelles technologies de traitement de données comme MapReduce de Google, et son équivalent en version open source, Hadoop, créé sous l'impulsion de Yahoo. Elles permettent de gérer de bien plus grandes quantités de données qu'auparavant et – point important – il n'est pas besoin de ranger ces dernières de façon bien ordonnée ou dans des tables de base de données classiques. A l'horizon, se profilent de nouvelles technologies d'analyse de volumes considérables de données qui se passent de hiérarchies rigides et de l'homogénéité d'antan* ». Cukier Kenneth, Mayer-Schoenberger Viktor, *Big Data : La Révolution des Données est en Marche*, Robert Laffont, 20 février 2014, p. 18.

70 v. Suart Ward Jonathan, Barker Adam, *Undefined by Data: A survey of Big Data Definitions*, University of St Andrews, 20 September 2013 ; Gandomi Amir, Haider Murtaza, *Beyond the hype : Big data concepts, methods and analytics*, International Journal of Information Management, Volume 35, issue 2. April 2015, pp. 137-144 ; De Mauro Andrea, Greco Marco, *What is big data ? A consensual definition and a review of key research topics*, AIP Conference Proceedings 2015, pp. 97-104.

71 Concept reflétant la capacité des technologies à s'insérer dans les espaces urbains pour capter un ensemble de données permettant d'améliorer sa fiabilité, sa fluidité ou sa sécurité. v. Caragliu Andrea, *Smart Cities in Europe*, Journal of Urban Technology, Volume 18, 2011, pp. 65-82 ; Chourabi H. et al., *Understanding Smart Cities: An Integrative Framework,* 2012 45th Hawaii International Conference on System Sciences, Maui, HI, 2012, pp. 2289-2297.

72 Wavestone, *Smart Cities et mobilité : la France en pointe sur le marché stratégique des métros automatiques*, Communiqué de Presse, 26 avril 2017, disponible sur http://wellcom.fr/presse/wavestone/2017/04/smart-cities-et-mobilite-france-en-pointe-sur-marche-strategique-des-metros-automatiques/ (consulté le 01/09/17).

73 v. Murdoch Travis, Detsky Allan, *The Inevitable Application of Big Data to Health Care*, JAMA, 2013, 309(13), pp. 1351-1352.

74 v. Provost Foster, Fawcett Tom, *Data science and its relationship to Big Data and Data-Driven decision making*, Big Data vol. 1, Issue 1, February 13, 213, pp. 51-59.

75 Faghmous James H., Kumar Vipin, *A big data guide to understanding climate change: the case for theory-guided data science*, Big Data, volume 2, issue 3, September 15, 2014, p155-163.

Européens à l'avenir. Il ne faut donc pas, par une approche manichéenne, considérer l'innovation technologique comme uniquement porteuse d'un renouveau économique.

28. Il convient, dans le même temps, d'appréhender l'innovation numérique comme ce qu'elle est réellement : un nouvel outil apolitique ayant une dimension technique propre. Cela permettra d'apprécier ce que la technologie offre comme nouvelles opportunités pour protéger la vie privée, mais également les nouvelles occasions qu'elle procure aux responsables de traitements, qu'ils soient privés ou publics, afin d'y attenter.

29. Pour cela, on peut identifier en premier lieu la dotation croissante des forces étatiques en technologies de surveillance. Apres les deux lois d'orientation et de programmation pour la performance de la sécurité intérieure[76], la loi du 24 juillet 2015 relative au renseignement[77] et la loi du 3 juin 2016 renforçant la lutte contre le crime organisé[78] ont considérablement renforcé les moyens dont dispose l'Etat pour surveiller son territoire numérique. Ce mouvement législatif semble d'ailleurs transnational, puisque la Suisse[79], le Royaume Uni[80], l'Allemagne[81], ou même les Etats Unis[82] ont récemment décidé de légiférer dans ce domaine, donnant plus ou moins de garanties relatives au droit au respect de la vie privée. L'Europe participe à cet élan juridique, en harmonisant les procédures d'échanges d'informations en matière fiscale avec la directive 2014/107[83], avec la directive 2016/681[84] relative à

76 Loi n°2002-1094 du 29 août 2002, *d'orientation et de programmation pour la sécurité intérieure*, JORF du 30 août 2002, p14398, texte n°1 ; Loi n° 2011-267 du 14 mars 2011, *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n°0062 du 15 mars 2011, p. 4582, texte n°2.

77 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

78 Loi n°2016-737 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, texte n°1

79 v. Votation n°607 sur la loi fédérale du 25 septembre 2015 sur le renseignement, LRens.

80 v. Investigatory Powers Act 2016, published by the Home Office the 1st March 2016.

81 v.Stellungnahme des Bundesrates, Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, Deutscher Bundesrat: Drucksachen und Protokolle [BR-Drs.] 430/16 (Beschluss), Sept. 23, 2016.

82 USA Freedom Act of 2015, H.R.2048, Public Law n°114-23, 6 February 2015.

83 Directive 2014/107/UE du Conseil du 9 décembre 2014, *modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal*, Journal Officiel de l'Union Européenne n°L359, 16 décembre 2014, pp. 1-29. .

84 Directive 2016/681 du Parlement Européen et du Conseil du 27 avril 2016, *relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, Journal Officiel de l'Union Européenne n°L119, 4 mai 2016, pp. 132-149.

l'utilisation des données des dossiers passagers, ou encore avec la directive 2016/680 relative aux échanges de données d'enquêtes[85].

30. À la suite des révélations d'Edward Snowden[86] sur l'utilisation qui peut être faite de ces nouvelles techniques, la question de l'encadrement de ces pratiques s'impose d'elle-même. Il conviendra donc de détailler les outils dont disposent les autorités ainsi que les moyens de contrôle de leurs activités que le législateur a mis en place pour encadrer ces nouvelles pratiques régaliennes.

31. Toutefois, l'impact négatif de la technologie ne saurait refléter la totalité de son influence sur le droit au respect de la vie privée. Dans les mêmes documents d'Edward Snowden révélant la mainmise technologique de la NSA sur les infrastructures numériques, on trouve un certain nombre d'exemples dans lesquels les forces régaliennes sont en difficulté face à l'innovation numérique[87]. Avec l'essor de l'informatique, de nouvelles technologies de chiffrement sont aujourd'hui utilisées par certains services de communication pour garantir la sécurité des échanges. Celles-ci sont même devenues une part importante de la sécurité des données sur internet[88]. Dès lors, si l'on doit analyser l'impact de la technologie, il faut nécessairement intégrer le versant positif de celle-ci, celui permettant aux citoyens de se protéger avec plus d'efficacité des immixtions non désirées.

32. Ce second constat conduit logiquement à une interrogation : celle de l'efficacité du droit face à la technologie. En élevant des barrières numériques, l'individu ou les services sont capables de s'opposer à l'exécution des dispositions législatives relatives à l'accès à certaines informations. Le cas de l'Iphone du terroriste de Boston a d'ailleurs été fortement médiatisé sur ce point[89]. En l'espèce, le Federal Bureau of Investigation Américain souhaitait

85 Directive 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement de 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/JAII du Conseil*, JOUE, L 119/89, 4 mai 2016,

86 v. Greenwald Glenn, *Nulle Part où se Cacher*, JC Lattès, 14 mai 2014, 280 p.

87 Ibid.

88 v. Conseil National du Numérique, *Tribune : chiffrement et lutte contre le terrorisme, attention à ne pas se tromper de cible,* disponible sur https://cnnumerique.fr/tribune-chiffrement/ (consulté le 01/09/17).

89 O'Ryan Johnson, *FBI wants Iphone unlocked in Boston gang case*, Boston Herald, 15 mars 2016, disponible sur http://www.bostonherald.com/news/local_coverage/2016/03/fbi_wants_iphone_unlocked_in_boston_gang_case (consulté le 01/09/17).

obtenir les données chiffrées du téléphone d'un suspect, en demandant à la société ayant créé le logiciel de chiffrement de lui fournir un accès. Celle-ci refusa d'exécuter cette requête, arguant d'une impossibilité technique autant qu'éthique, décision validée par la Cour de justice Californienne[90]. Si le cas ne s'est pas encore présenté en France, l'analyse de ce nouveau type de technologie sur le plan juridique est nécessaire, notamment dans la perspective de la mise en place généralisée de la Privacy By Design[91].

33. Selon le règlement général sur la protection des données : « *afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer* »[92]. En intégrant une obligation de protéger les données, sans indiquer de technologie précise, le législateur Européen a offert la faculté aux responsables de traitement d'utiliser de puissants algorithmes de chiffrement pouvant, par la suite, limiter la capacité des services Etatiques à prendre connaissance des données. Dans ce contexte, la définition technique de ces moyens de protection sera déterminante pour le futur de l'applicabilité du droit.

34. Toutefois, il convient de rappeler que si les aspects techniques sont une part importante de notre étude, nous ne pourrons rentrer dans le détail des normes applicables à la sécurité des systèmes d'informations, et donc des données, telles que les normes ISO 13335[93],

90 United States District Court for the Central District of California. *Order compelling Apple Inc. to assist Agents in Search,* Retrieved February 27, 2016.

91 Concept développé par Ann Cavoukian. v. Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, December 2012, 74 p.

92 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, considérant 78.

93 ISO/IEC 13335-1:2004, Technologies de l'information, Techniques de Sécurité, Gestion de la sécurité des technologies de l'information et des communications, norme annulée par la norme ISO/IEC 27000.

ISO 15408[94], ISO 27001[95], ISO 27002[96] et ISO 27018[97]. De même, il ne sera pas question de comparer la sécurité ou la fiabilité des différents algorithmes de chiffrement des données tels qu'AES[98], HTTPS[99] ou RSA[100]. En effet, la seule possibilité que des techniques existantes réduisent les prérogatives régaliennes d'accès aux données est indicative d'une obstruction potentielle de la technologie à l'applicabilité du régime. Dès lors, il ne nous appartient pas d'en décrire le fonctionnement interne, mais de comprendre les mécanismes juridiques qui régissent leurs déploiements ou leurs utilisations. Ainsi, si des éléments techniques seront évoqués, ils ne le seront qu'en tant que technologies nommées ou définies par la législation.

35. Enfin, un dernier élément contextuel devra être pris en compte : la dimension ubiquitaire de l'innovation numérique. Lorsqu'un utilisateur Européen confie ses données à un service, celles-ci peuvent être stockées ou traitées à des milliers de kilomètres de son lieu d'accès. De la même manière, lorsqu'il est victime d'une atteinte, le responsable peut se trouver dans un autre Etat. Le juriste sera donc amené à s'interroger non pas sur la pertinence de l'existence de la technologie offrant une telle possibilité, mais sur l'applicabilité de normes territorialisées dans un espace transnational. L'exemple de la récente remise en cause de la validité du Safe Harbour[101], et la renégociation de son successeur, le Privacy Shield[102], reste emblématique de cette problématique. En l'espèce, la polémique entourant la révocation de cet accord régissant les transferts de données entre l'Union Européenne et les Etats Unis fait suite aux révélations d'Edward Snowden sur la surveillance effectuée par la NSA sur les données. Mais selon la décision de la Cour Européenne, l'annulation repose principalement sur un simple fait : « *la Commission n'a pas fait état, dans la décision 2000/520, de ce que les*

94 ISO/IEC 15408-1:2009, Technologies de l'information, Techniques de Sécurité, Critères d'évaluation pour la sécurité T1, publiée en décembre 2009.

95 ISO/IEC 270001 :2013, Technologies de l'information, Techniques de Sécurité, Systèmes de management de la sécurité de l'information, Exigence, publiée en octobre 2013.

96 ISO/IEC 270002 :2013, Technologies de l'information, Techniques de Sécurité, Code de bonne pratique pour le management de la sécurité de l'information, publiée en Octobre 2010.

97 ISO/IEC 270018 :2014, Technologies de l'information, Techniques de Sécurité, Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII, publiée en août 2014.

98 Advanced Encryption Standard, v. Nechvatal James et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, U.S. Department of Commerce, 2 October 2000.

99 v. Walls Colin, *Embedded Software: The Works*, Newnes, 18 octobre 2005, 416 p.

100 v. Mutyaba Robert, *Improving the RSA Cryptographic Algorithm*, Lambert Academic Publishing, 2010, 84 p.

101 CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14.

102 Commission Européenne*, La Commission Européenne présente le paquet « bouclier de protection des données UE-Etats-Unis » : des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données*, IP/16/433, Bruxelles, 29 février 2015.

Etats-Unis d'Amérique « assurent » effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux »[103]. Ce point d'achoppement est justement celui de l'application des dispositifs de protection du traité qui étaient en contradiction avec la législation Etats-Unienne autorisant l'accès aux données par les services de renseignement. Par conséquent, notre étude intégrera également une prise en compte de la dimension internationale des échanges de données.

36. En résumé, l'approche contextuelle semble indiquer que le droit au respect de la vie privée s'inscrit dans un mouvement économique et technologique transnational particulièrement dépendant des conditions de licéité de la valorisation des données à caractère personnel. En cela, il devient le principal vecteur de sécurité juridique pour l'innovation numérique, et en corollaire, il influence directement le devenir de celle-ci. Or, à ces objectifs s'oppose celui d'une protection forte du droit au respect de la vie privée dans l'innovation numérique, qui serait particulièrement contraignante pour l'industrie et les Etats. Dans cet environnement, la confrontation entre l'innovation et le droit au respect de la vie privée ne permet que difficilement d'obtenir une protection efficace par manque de symbiose. Les utilisateurs peuvent, en demandant un contrôle excessif sur leurs données, freiner une innovation potentiellement porteuse de solutions pour l'avenir. À l'inverse, l'industrie peut voir dans une protection trop restrictive une menace pesant sur son modèle économique. Par conséquent, nous chercherons dans cette étude à aller au-delà de cet antagonisme trop souvent réducteur, pour évaluer puis définir une protection qui soit à la fois efficace pour les citoyens et respectueuse de l'innovation. Il ne s'agira pas simplement de cataloguer les mesures juridiques actuelles où envisageables pour protéger un concept de vie privée redéfini, mais bien d'analyser, dans le même temps, le rôle catalyseur de l'innovation pour sublimer ou menacer cette protection.

103 CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14, point 97.

Périmètre de l'étude

37. En définissant le contexte juridique sous l'angle économique, technologique et transnational, deux éléments importants semblent manquer : la dimension sociale et la dimension politique du droit au respect de la vie privée et du régime applicable aux données à caractère personnel.

38. On peut rappeler de manière liminaire que la conceptualisation de la vie privée dépasse le droit, l'économie ou la technologie, et que les considérations phénoménologiques[104], sociales[105] ou même religieuses[106] peuvent apporter des éléments de réponse quant à son essence.

---

104 Concernant la définition de la vie privée par sa dimension phénoménologique, on peut citer l'analyse de Gilles Deleuze dans *Empirisme et Subjectivité*, PUF, 13 octobre 2010, 160 p.; les concepts développés par Martin Heidegger dans *Etre et Temps*, Gallimard, 12 novembre 1986, 600 p. Notamment à travers celui de *Dasein* ; ou encore Emmanuel Kant dans *Critique de la Raison Pure*, Flammarion, 18 août 2006, 749 p., qui partage l'idée de *schématisme* avec David Hume, exprimée dans *Traité de la Nature Humaine : Livre 1 et appendice, l'Entendement*, Flammarion, 4 janvier 1999, 433 p.

105 v. Note de bas de page n°6.

106 Concernant la définition de la vie privée par la religion, on peut citer l'étude de l'abbé F.B. Clément, dans Clément F.B., *Philosophie Sociale de la Bible*, Paul Mellier Editeur, 1848, p. 274, qui semble démontrer une nécessaire fusion de la pensée individuelle du croyant avec celle de l'interprétation dominante de la Bible : *« [Le libre interprète] est conduit forcément à prendre la certitude subjective pour la certitude objectif, c'est-à-dire que sa dernière conclusion est celle-ci : « je crois à la parole divine, parce qu'elle est conforme à ma pensée ». Veut-il en effet, prendre la Bible comme règle de sa pensée ; il ne la connait pas encore, cette Bible, tant qu'il ne l'aura pas interprétée : il ne peut donc lui emprunter un terme de comparaison certain avec lequel il confrontera sa pensée. En dehors de ce livre il ne possède que sa raison privée, sa pensée individuelle, et, en prétendant chercher dans le livre saint un pensée divine, il n'y cherchera réellement que la sienne […] Le libre interprète est donc un homme abandonné dans la main de son conseil. [Or] quand le Créateur plaça le premier homme dans cette position, ce ne fut pas sans lui donner toutes les lois nécessaires, appropriées à sa nature et à ses besoins, il lui imposa des commandements et des préceptes qui devraient le conserver, à condition qu'il garderait toujours la foi* ». Dans ce contexte, les préceptes des textes sacrés définissent la manière dont chacun peut vivre sa vie, faisant reculer d'autant la liberté de la vie privée. On peut constater cette problématique avec l'impact de la région Musulmane sur la manière dont les croyants peuvent se vêtir. Cela fut d'ailleurs observé sous l'angle juridique, notamment dans la décision de la CEDH dans l'affaire n°37798/13, *Belcacemi et Oussar c. Belgique*, du 11 juillet 2017, dans laquelle la Cour déclare : « *l'interdiction de porter dans l'espace public une tenue destinée à dissimuler le visage posait des questions tant au regard du droit au respect de la vie privée des femmes qui souhaitent porter le voile intégral pour des raisons tenant à leurs convictions qu'au regard de leur liberté de manifester celle-ci. Cela étant dit, pour autant que cette interdiction est mise en cause par des personnes qui, telles que les requérantes en l'espèce, se plaignent d'être en conséquence empêchées de porter dans l'espace public une tenue que leur pratique d'une religion leur dicte de revêtir, il y a lieu d'examiner cette partie de la requête en mettant l'accent sur la liberté garantie par l'article 9 de la Convention de chacun de manifester sa religion ou ses convictions* ». On peut également citer l'arrêt de la CEDH n°43835/11, *S.A.S. c. France*, 1er juillet 2014, n°43835/11, dans laquelle la Cour déclare qu'elle : « *peut comprendre le point de vue selon lequel les personnes qui se trouvent dans les lieux ouverts à tous souhaitent que ne s'y développent pas des pratiques ou des attitudes mettant fondamentalement en cause la possibilité de relations interpersonnelles ouvertes qui, en vertu d'un consensus établi, est un élément indispensable à la vie collective au sein de la société considérée. La Cour*

39. Selon Pierre Demeulenaere : « *la théorisation de l'émergence d'une société reposant sur des droits individuels accompagne la formalisation effective de tels droits individuels (sans que des relations de cause à effet puissent être unilatéralement établies dans une direction ou dans une autre). L'individualisation se produit face aux droits d'une « communauté », quel que soit d'ailleurs le sens exact attaché à cette notion. Le droit à la vie privée s'inscrira dans la continuité d'une telle revendication de droits individuels (conçus ou non comme naturels)* »[107]. Il faudrait donc rechercher la définition primaire de la vie privée dans les conditions de formation d'une telle société. Dans ce contexte, pour Isabelle Berrebi-Hoffmann et Arnaud Saint-Martin : « *les sciences sociales sont bien placées pour analyser des catégories en cours de redéfinition : l'intime, le privé, le commun et le public, qui sont aujourd'hui brouillées et varient d'une tradition nationale à l'autre, d'un espace de discussion à l'autre. D'où l'utilité d'aborder l'histoire et les modalités contemporaines de la recomposition des frontières entre l'Etat et le particulier, le public et le privée, l'intime et le politique et de penser les lieux ou ces catégories achoppent et sont façonnées mutuellement* »[108].

40. En suivant cette analyse, une étude portant sur la vie privée et le numérique devrait nécessairement intégrer, dans une perspective sociale, les nouveaux comportements qu'engendre la numérisation de nos échanges quotidiens[109]. Mais une telle prise en compte aurait pour effet d'étendre indéfiniment le spectre de notre analyse alors même qu'il ne s'agit que d'une étude juridique. Pour cette raison, les aspects sociaux et religieux, sans minimiser leur importance, ne seront évoqués que partiellement.

---

peut donc admettre que la clôture qu'oppose aux autres le voile cachant le visage soit perçue par l'État défendeur comme portant atteinte au droit d'autrui d'évoluer dans un espace de sociabilité facilitant la vie ensemble », et donc par corolaire, porter atteinte au droit au respect de la vie privée des personnes évoluant de ces espaces publics.

107 Demeulenaere Pierre, *Les Difficultés de la Caractérisation de la Notion de Vie Privée d'un Point de Vie Sociologique*, La Protection de la Vie Privée dans la Société de l'Information, Chapitre 11, p. 194.

108 Berrebi-Hoffmann Isabelle, Saint-Martin Arnaud, *Vie Privée et Démocratie, un Couple en Tension*, Socio, 7, 2016, p. 7.

109 On peut prendre exemple sur l'étude de Claire Balleys et Sami Coll sur les changements des rapports qu'ont les adolescents à travers l'utilisation des outils numériques, v. Balleys Claire, Coll Sami**,** *La Mise en Scène de la Vie Privée en Ligne par les Adolescents*, *RESET*, 2015, disponible sur http://reset.revues.org/547 (consulté le 01/09/17).

41. Le même raisonnement est applicable à la question de l'intégration de la dimension politique dans l'analyse du régime juridique. S'il faut reconnaitre que dans un contexte doublement marqué par une volonté de croissance économique[110] et par la vague d'attentats terroristes perpétrés sur le sol Français[111], le sujet de la licéité de l'utilisation des données à caractère personnel ne saurait être d'une neutralité politique absolue. Cette étude n'est pas celle de l'idéologie qui marque le droit au respect de la vie privée et sa traduction dans la société de l'information. Nous nous détachons en cela de l'approche retenue par le Conseil National du Numérique lorsqu'il déclare que: « *plus que jamais les technophobes et les technolâtres doivent être renvoyés dos à dos et il s'agit de concevoir le numérique comme ce qu'il est : un facteur de bouleversements importants auxquels il faut donner un sens, une direction et des valeurs. La société numérique n'est pas une force qui va, mais procède au contraire d'un ensemble de choix individuels, mais aussi et surtout collectifs* »[112]. Car en proposant de donner *un sens, une direction et des valeurs*, à travers un choix qui serait *surtout collectif*, nous ne ferions que souligner l'aspect idéologique qui accompagne le mouvement législatif. Ce faisant, nous invaliderions, par l'expression de notre propre idéologie, toute tentative d'analyse objective de l'efficacité juridique du régime à protéger le droit au respect de la vie privée dans l'innovation numérique.

42. Pour éviter un tel écueil, le sujet de la modification des modalités d'attribution de compétence des autorités nationales indépendantes par le règlement général sur la protection des données[113] ne sera que partiellement évoqué. En effet, en introduisant le concept d'une

110 « *Le numérique et ses usages sont au cœur d'un mouvement de transformation profonde de la société et de l'économie, qui concerne tous les secteurs d'activité et représenterait environ le quart de la croissance française* », Coutelle Catherine, *Rapport d'information n°3318 fait au nom de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes sur le projet de loi pour une République numérique*, Enregistré à la Présidence de l'Assemblée nationale le 15 décembre 2015, p. 4.

111 On peut mentionner succinctement les attentats du 13 novembre 2015, du 14 juillet 2016 à Nice, du 26 juillet 2016 à Saint-Etienne-du-Rouvray.

112 Conseil National du Numérique, *Rapport Ambition Numérique : Pour une politique Française et Européenne de la transition numérique*, Rapport remis au Premier Ministre, Juin 2015, p. 19.

113 « *«données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;* ». 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

autorité de contrôle « *chef de file* »[114], le règlement a offert aux responsables de traitement la faculté de s'adresser à un interlocuteur unique au niveau Européen, celui de l'Etat où est installé leur établissement principal. Pour Nathalie Martial-Braz, « *il peut sembler contestable dès lors qu'il pourrait autoriser, implicitement, une sorte de forum shopping, à l'initiative des responsables de traitement ou des sous-traitants, et ce en faveur d'Etats membres dans lesquels les autorités de régulation seraient jugées, à tort ou à raison, plus clémentes* »[115]. Mais plus encore selon Mihaela Ailincai, la possibilité d'utiliser la règlementation comme une autorisation implicite de forum shopping « *aboutirait à terme à une concentration de la régulation entre les mains de quelques autorités de contrôle, qui ne seraient pas nécessairement celles dont les ressources seraient les plus développées, ce qui pourrait aggraver encore leur situation et provoquer un cercle vicieux* » [116].

43. Pour autant, de telles considérations, aussi justes soient elles, vont à l'encontre de l'analyse juridique structurelle qui considère le règlement Européen comme un instrument législatif d'application directe et uniforme [117]. Seuls les critères de définitions des modalités de licéité des traitements par les autorités indépendantes ou contenus dans le règlement peuvent être l'objet de notre analyse. Le périmètre de notre étude restera donc centré sur les aspects juridiques factuels du droit au respect de la vie privée, pour apprécier de manière scientifique et objective sa translation dans le régime applicable aux données à caractère personnel, sans s'attacher aux implications politiques afférentes.

44. Enfin, une telle analyse, même juridique, perdrait de son intérêt si celle-ci cherchait à passer en revue l'ensemble des dispositifs législatifs ou règlementaires applicables en la matière. Pour cette raison, la modification récente du régime applicable aux données de santé par la loi du 26 janvier 2016[118] ne sera que partiellement évoquée malgré son importance[119],

114 Ibid, articles 55 et suivants.

115 Martial-Braz Nathalie, *L'Extraterritorialité des Décisions des Autorités de Régulation : Gage d'Efficacité de la Protection des Données Personnelles en Europe,* Colloque : La coopération policière, douanière et judiciaire en Europe, Besançon, 24 septembre 2015, p. 188.

116 Ailincai Michaela, *Espoirs et Inquiétudes Autour de la Révision du Cadre Juridique Général de l'Union Européenne sur la Protection des Données à Caractère Personnel*, Revue de l'Union Européenne n°576, mars 2014, p. 170.

117 « *Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout état membre* ». Version consolidée du traité sur le fonctionnement de l'Union européenne, Journal Officiel de l'Union Européenne n°C115/47, 9 mai 2009, article 288.

118 Loi n°2016-41 du 26 janvier 2016, *de modernisation de notre système de santé*, JORF n°0022 du 27 janvier 2016, texte n°1.

119 Dans les changements importants concernant les données, on peut citer brièvement : l'évolution des

de même que les récentes évolutions de la doctrine de la CNIL concernant l'appréciation des technologies biométriques qui constitue un objet d'étude à part entière[120]. En effet, si ces deux pans de la législation s'appliquent à des données dont les régimes divergent sur des aspects techniques, la philosophie de la licéité de leurs traitements reste extrêmement proche de celle du régime général. De même, seul le droit Français et Européen, à l'exception de quelques éléments externes de références, seront discutés.

Problématique de l'étude et annonce de plan

45. À la lumière du changement de paradigme engendré par l'innovation numérique au regard du droit au respect de la vie privée, seule une analyse de type phénoménologique peut apprécier la pertinence de la protection accordée aux données à caractère personnel. La question à laquelle nous devrons répondre est celle de savoir dans quelle mesure la vie privée est prise en compte dans l'innovation technologique, et si cette prise en compte est suffisante dans les conditions actuelles d'utilisation des données par les Etats et par les entités privées.

---

modalités de partage de données de santé pour l'équipe de soin, définie par l'article L110-12 du Code de la Santé Publique comme : « *un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte de diagnostic, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes [..]* », ainsi que celles concernant le personnel hospitalier avec la modification de l'article L1110-4 du même code, par Ordonnance n°2017-31 du 12 janvier 2017 *de mise en cohérence des textes au regard des dispositions de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé,* JORF n°0011 du 13 janvier 2017, texte n°25 ; de même que la mise en place du dossier médical partagé et d'un ersatz de droit à l'oubli face à l'assurance emprunteur par le décret n°2017-173 du 13 février 2017 *précisant les modalités d'information des candidats à l'assurance-emprunteur lorsqu'ils présentent du fait de leur état de santé ou de leur handicap un risque aggravé*, JORF n°0038 du 14 février 2017, texte n°8.

120 Pour cela, il faut mesurer l'évolution de la doctrine de la Commission depuis 2006, avec une première distinction des technologies dites « *à trace* » et « *sans trace* » et sa refonte avec la publication de la nouvelle grille d'analyse de risque des technologies biométriques le 30 juin 2016. v. Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-186 du 30 juin 2016 *portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maitrise par la personne concernée sur son gabarit biométrique*, AU-052, JORF n°0225 du 27 septembre 2016, texte n°53 ; Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-187 du 30 juin 2016 *portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable de traitement*, AU-053, JORF n°0225 du 27 septembre 2016, texte n°52

46. Dans un premier temps, il faudra observer l'adaptation du droit au respect de la vie privée au phénomène technologique (Partie I). Cette analyse permettra de comprendre la manière dont le droit au respect de la vie privée se conçoit, définition à laquelle nous opposerons sa translation dans le monde numérique à travers le régime applicable aux données à caractère personnel. De même, il sera nécessaire de qualifier l'applicabilité du régime dans un environnement technique qui semble, parfois, le dépasser.

47. Dans un second temps, nous observerons de quelle manière les acteurs de l'innovation numérique se sont adaptés au régime protecteur des données à caractère personnel (Partie II). De fait, en centrant le régime de protection sur le consentement de l'utilisateur, le législateur a entrainé un phénomène croissant de contractualisation des échanges entre les utilisateurs et les différents services numériques, à l'intérieur desquels les conditions d'utilisation des données prennent une place prépondérante. Il nous appartiendra d'analyser cette libéralisation de l'usage des données à caractère personnel dans le contexte du droit au respect de la vie privée.

PARTIE I

L’adaptation du droit au respect de la vie privée à un phénomène technologique

*

48. L'innovation technologique a créé une rupture dans la conception du droit au respect de la vie privée. Selon le rapport des Sénateurs Yves Détraigne et Anne-Marie Escoffier : « *de résolutions de difficultés en solutions, le législateur a œuvré pour que la notion de vie privée, intégrée depuis la philosophie des Lumières à notre patrimoine historique, culturel et identitaire, reste, dans notre société démocratique, indissociable de l'existence de l'individu et de l'exercice des libertés : la société reconnaît à l'individu le droit de disposer d'un espace privé, distinct de la vie collective de la communauté. Comment, dès lors, concilier les nouveaux pouvoirs que font peser sur chaque individu les nouvelles technologies avec ce droit à la vie privée ? Comment éviter que des institutions, publiques ou privées, ou même des individus n'utilisent ces formidables « mémoires numériques » au détriment de notre vie privée pour porter atteinte à nos libertés et à notre capacité d'autodétermination ?* »[121].

49. Cette question de l'adaptation du droit au respect de la vie privée à un phénomène technologique est déterminante pour notre étude. D'une part parce qu'elle nécessite de définir avec précision ce qui est l'essence du droit au respect de la vie privée. D'autre part parce qu'elle demande une prise en compte des capacités technologiques actuelles afin d'être en mesure d'apprécier l'efficacité de la réponse législative face à ce nouveau type d'atteinte.

121 Détraigne Yve, Escoffier Anne-Marie, *Rapport d'information n°441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Annexe au procès-verbal de la séance du 27 mai 2009, p. 7.

50. Car il s'agit bien d'une nouvelle forme d'atteinte. Toujours selon le rapport : « *Il nous faut être conscients, nous, homo sapiens devenus « homo numericus », du risque qui nous guette d'être pris au piège des mémoires numériques qui jouent le même rôle que notre propre mémoire : toujours présentes, même si elles paraissent enfouies au plus profond d'un système dont nous ne pouvons pas mesurer l'envergure, elles sont là dans une posture qui peut nous porter alternativement de la progression à la régression selon l'usage que nous en faisons. Il nous revient donc d'être ces veilleurs vigilants face aux grands enjeux « informatique et liberté » pour que le respect de la personne humaine, de sa vie privée et de sa dignité reste toujours un principe absolu* » [122].

51. Il conviendra donc d'analyser comment le législateur a choisi de définir l'encadrement juridique de cette nouvelle forme d'atteinte à la vie privée que semble constituer l'innovation technologique (Titre I) ; avant de pouvoir déterminer l'efficacité de celui-ci à s'appliquer dans un contexte technologique (Titre II).

122 Détraigne Yve, Escoffier Anne-Marie, *Rapport d'information n°441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Annexe au procès-verbal de la séance du 27 mai 2009, p. 7.

Titre I

L'encadrement juridique d'une nouvelle forme d'atteinte à la vie privée

*

52. Selon Christiane Féral-Schuhl, évoquant la déclaration de Bill Gates dénonçant dès 1997 le fait que « *des entreprises du secteur privé et des administrations (qui) possèdent déjà une masse d'information sur notre compte [Et que] nous n'avons aucune idée de la manière dont elles l'utilisent et si elle est exacte* »[123], nous sommes en droit de nous demander si « *dans cette société où les technologies omniprésentes offrent au citoyen une visibilité permanente, on peut revendiquer un droit à la vie privée à l'ère numérique ?* »[124].

53. Pour répondre à ce questionnement, il faut d'abord définir avec précision ce que l'on entend par « *droit à la vie privée* », avant d'examiner ce que celui-ci est devenu dans la société de l'information. Pour cela, avant d'évoquer ce qu'est la protection de la vie privée numérique par le régime applicable aux données à caractère personnel (Chapitre II), nous chercherons à comprendre quel est le périmètre protecteur du droit au respect de la vie privée (Chapitre I).

123 v. Gates Bill, *La Route du Future*, Pocket, 2 janvier 1997, 332 p.

124 Féral-Schuhl Christiane, *Peut-on protéger la vie privée à l'heure du numérique ?,* publié le 27 avril 2015, disponible sur http://www.feral-avocats.com/fr/publication/peut-on-proteger-la-vie-privee-a-lheure-du-numerique/ (consulté le 01/09/17).

Chapitre I

La protection offerte par le droit au respect de la vie privée

*

54. Bien qu'étant l'un des concepts fondamentaux du droit, le droit au respect de la vie privée n'a jamais fait l'objet d'une définition positive identifiant de manière exhaustive ses éléments intrinsèques.

55. Une définition de son périmètre exact ne saurait se trouver dans la jurisprudence Européenne. En effet, pour les juges de Strasbourg, il n'est « *ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de ''vie privée''* »[125]. Il serait même restrictif de *« la limiter à un cercle intime où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle »*[126] alors que *« le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables* »[127]. La Cour examine donc au cas par cas les affaires qui lui sont présentées, en s'appuyant sur l'article 8 de la Convention Européenne des Droits de l'Homme et des libertés fondamentales, qui juxtapose les notions de vie privée et familiale, de domicile et de correspondance sans les définir avec précision[128].

125 CEDH, 16 décembre 1992, *Niemietz c. Allemagne*, n°13710/88, considérant 29.
126 Ibid.
127 Ibid.
128 Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4,XI, 1950, article 8.

56. Le droit interne ne pallie pas non plus cette absence. Le législateur Français a choisi la même approche avec la loi du 17 juillet 1970[129] qui a introduit le concept de vie privée à l'article 9 du Code Civil, rappelant simplement que « *chacun a droit au respect de sa vie privée* », sans circonscrire la notion. Néanmoins, certains éléments ont été définis avec plus de précision. Les articles 226 et suivants du Code Pénal visent des infractions telles que la captation, l'enregistrement ou la transmission, sans le consentement de leur auteur, des paroles et de l'image d'une personne[130]. Celles-ci sont complétées par des dispositions spécifiques à chaque secteur juridique, comme l'accès au domicile[131] ou à la correspondance[132], tout en restant en périphérie d'une définition holistique de la vie privée.

57. Ainsi, bien qu'hétéroclites, ces éléments pris dans leur ensemble contribuent à construire un portrait pointilliste de la vie privée. Mais l'image obtenue ne permet que de dessiner un halo autour de la notion, sans parvenir à la réduire à un concept défini. Selon la formule de Robert Badinter : « *s'agissant de la vie privée, […] plutôt que de définir le contenu, les juristes Français se sont plus volontiers attachés à dépeindre le contenant. Depuis Royer-Collard, le célèbre mur de la vie privée se découpe bien nettement sur l'horizon juridique, mais quant au domaine qu'il enclot, ses dimensions s'avèrent singulièrement variables* » [133]. Dès lors, si la vie privée se conçoit sous différentes acceptions, réunissant la nécessité de protéger des aspects particuliers de la vie sociale des individus mais aussi des lieux d'usages ou des moyens d'expression sans pour autant se fermer à l'intégration d'autres éléments, l'absence de définition entraîne une insécurité juridique.

58. Par exemple, il « *est admis depuis longtemps en jurisprudence que des lettres, qui dans d'autres domaines du droit, seraient écartées comme violant le secret des correspondances, puissent être utilisées en matière de divorce pour prouver les fautes, et notamment l'adultère, à la condition que les lettres aient été obtenues sans violence ni fraude* »[134]. Les juges du fond établissent ici une distinction de l'appréciation du périmètre

129 Loi °70-643 du 17 juillet 1970*, tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 19 juillet 1970 p. 6751.
130 Code Pénal, article 226-1et 226-2.
131 Code Pénal, article 226-4.
132 Code Pénal, article 226-15.
133 Badinter Robert, *Le Droit au Respect de la Vie privée*, JCP G 1968, I, 2136, n°22.
134 Cour de Cassation, Rapport 2010, La Documentation Française, 2011, Paris, p. 250.

protecteur de la vie privée en fonction de la difficulté à produire une preuve[135]. Le droit au respect de la vie privée ne serait donc pas une notion fixe, mais resterait dépendante du contexte dans lequel elle est invoquée. Dans une telle perspective, il paraitrait donc normal que celle-ci puisse évoluer à travers le temps, en fonction des besoins ou des époques, jusqu'à disparaitre totalement si cela était nécessaire.

59. Or, dans ce nouvel environnement numérique où l'information sur les personnes relève directement de ce qui nous semble être l'essence de la vie privée, il est nécessaire de pallier cette absence de définition générale qui s'avère préjudiciable pour les citoyens. Ceci servira, dans le même temps, à fixer un point d'observation pour évaluer l'efficacité de la protection de la vie privée numérique par rapport à celui offert à la vie privée.

60. Pour cela, nous devons commencer par analyser les caractéristiques que la jurisprudence prête à cette notion. Ainsi, la décision du 15 mai 1970 de la Cour d'Appel de Paris, définit le droit au respect de la vie privée comme le « *droit pour une personne d'être libre de mener sa propre existence comme elle l'entend avec le minimum d'ingérences extérieures* »[136]. Il y a là une double reconnaissance, d'abord celle d'une volonté individuelle (« *libre de mener sa propre existence* »), puis celle d'une protection de son expression (face aux « *ingérences extérieures* »). Mais à la racine de cette individualisation, la Cour place la notion de liberté, comme consubstantielle à la capacité de décision et d'action.

61. Cette association entre liberté et vie privée n'est pas unique dans la jurisprudence. Peu présent dans la jurisprudence Constitutionnelle avant la loi du 17 juillet 1970[137], le droit au respect de la vie privée a fait l'objet d'une reconnaissance parcellaire avant d'être progressivement élevé au rang de droit fondamental par la doctrine à partir la notion de liberté. Ainsi, dans sa décision du 12 Janvier 1977, le Conseil Constitutionnel remplaçait sa mention par la notion de liberté individuelle lorsqu'il s'agissait d'évaluer l'impact d'une fouille de véhicule sur les droits des citoyens[138]. Cette logique d'assimilation continua, lorsque le Conseil considéra que « *la prévention d'atteintes à l'ordre public, notamment*

135 Cass. Civ., 26 Novembre 1975, n°74-10034, Bull. 1975, II, n°314, p. 289.
136 CA. Paris, 7eme chambre, 15 mai 1970.
137 Loi °70-643 du 17 juillet 1970*, tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 19 juillet 1970 p. 6751.
138 Conseil Constitutionnel, Décision n°76-75 du 12 janvier 1977, Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales.

d'atteintes à la sécurité des personnes et des biens, et la recherche des auteurs d'infractions, sont nécessaires à la sauvegarde de principes et droits à valeur constitutionnelle ; 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 ; que la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle »[139].

62. D'un point de vue constitutionnel, cette approche crée une situation de dépendance de différents droits subjectifs au droit au respect de la vie privée. Ainsi, comme le résume la décision du Conseil Constitutionnel en date du 23 juillet 1999 : « *la liberté proclamée par (l'article 2 de la déclaration des droits de l'homme et du citoyen) implique le respect de la vie privée* »[140]. Dès lors, pour Yves Poullet et Antoinette Rouvroy, le droit au respect de la vie privée est « *l'instrument des capacités de développement personnel autonome, qui sont, dans une société donnée et à une époque donnée, nécessaires au fonctionnement démocratique du régime politique en vigueur* »[141]. En cela, il permet « *d'expliquer le fondement de toutes les autres libertés. C'est ainsi qu'avec raison, H. Burkert peut écrire que le droit à la vie privée est, parmi les autres libertés, la liberté fondamentale fondamentale*[142]*, c'est-à-dire doublement fondamentale en ce sens qu'elle constitue la possibilité de toutes les autres libertés fondamentales »*[143].

63. Ainsi, le droit au respect de la vie privée peut se concevoir comme une protection de la faculté d'autonomisation d'un individu, auquel on accorde ensuite un périmètre décisionnel identifié. Notons, à ce stade, qu'il s'agit d'un véritable choix sémantique, afin de distinguer notre réflexion de celle ayant trait à l'autonomie décisionnelle[144]. La faculté d'autonomisation

139 Conseil Constitutionnel, Décision N° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 - Journal officiel du 21 janvier 1995, p. 1154, considérant 3.

140 Ibid.

141 Poullet Yves, Rouvroy Antoinette, *Le Droit à l'Autodétermination Informationnelle et la valeur du développement personnel. Une Réévaluation de l'importance de la vie privée pour la démocratie*, Etat de Droit et virtualité, Ed. Karim Benyekhlef & Pierre Trudel, Montréal: thémis, 2009, p. 161.

142 Ibid, p. 177. Citant : Burket H, *Dualities of Privacy – An Introduction to « Personal Data Protection and Fundamental Rights »*, dans M.V. Perez, A. Palazzi, Y. Poullet (eds), Privacy – New Visions, Cahier du Crid, n°31,2008, pp. 13-23.

143 Burket H, *Dualities of Privacy – An Introduction to « Personal Data Protection and Fundamental Rights »*, dans M.V. Perez, A. Palazzi, Y. Poullet (eds), Privacy – New Visions, Cahier du Crid, n°31,2008, pp. 13-23.

144 Notion d'autonomie décisionnelle que l'on peut retrouver notamment dans les travaux d'Yves Poullet et Antoinette Rouvroy, Op. Cit.

permet de rendre compte du cheminement interne de la pensée humaine, de son développement jusqu'à la conceptualisation de la réalisation future d'une action, permettant d'éviter l'écueil de l'instantanéité de l'examen de l'existence d'une autonomie décisionnelle. En effet, il ne s'agit pas de savoir si à un instant donné la personne est libre d'effectuer un choix, mais si tous les éléments externes de son développement personnel ont été réunis afin que celle-ci puisse l'effectuer librement. Avec cette prise de position, nous retrouvons bien les deux notions identifiées par la Cour d'Appel de Paris[145], volonté individuelle et protection contre l'ingérence extérieure, en l'absence desquelles les possibilités d'exercice des libertés fondamentales sont entamées.

64. Cette définition permet également de palier la faiblesse de la définition de vie privée en termes de sphères intimes. De fait, si l'on considère que le domicile fait partie de la sphère intime d'une personne, on réduit la notion de vie privée à un enclos physique. En prenant l'exemple du lit conjugal, on pourrait aisément comprendre que l'immixtion externe constituerait une violation de cette sphère. Pourtant dans cet exemple, on ne pourrait nier qu'une absence d'éducation sexuelle, qui « *contribue à l'apprentissage responsable, dans le respect de soi et des autres* » selon le Ministère de l'éducation[146], peut restreindre la vie privée d'une personne, bien qu'il n'y ait pas d'immixtion dans la « *sphère* » doctrinale. De même, la Cour Européenne indique que c'est la protection de la volonté de personne[147] qui justifie une intervention jusque « *dans le domaine des relations sexuelles, qui est l'un des plus intimes de la sphère privée* » [148]. Ainsi, bien que « *la faculté pour chacun de mener sa vie comme il l'entend peut également inclure la possibilité de s'adonner à des activités perçues comme étant d'une nature physiquement ou moralement dommageables ou dangereuses pour sa personne. […] La notion d'autonomie personnelle peut s'entendre au sens du droit d'opérer des choix concernant son propre corps* » [149].

145 CA. Paris, 7eme chambre, 15 mai 1970.
146 Site internet du Ministère de l'éducation, *La santé des élèves,* disponible sur http://www.education.gouv.fr/cid50297/la-sante-des-eleves.html#%C3%89ducation%20%C3%A0%20la%20sexualit%C3%A9 (consulté le 22/02/2017).
147 CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, n° 42758/98 et 45558/99.
148 CEDH, 27 septembre 1999, *Smith et Grady c. Royaume-Uni*, n°33985/96 et n°33986/96, para. 89.
149 CEDH, 29 juillet 2002, *Pretty c. Royaume Uni*, n° 2346/02, para. 66.

65. Dès lors, le droit au respect de la vie privée consacré par l'article 8 de la Convention Européenne des droits de l'homme, qui intègre la notion de développement personnel[150], ne peut se résumer à une sphère de protection. Il s'agit bien d'une faculté d'autonomisation à laquelle on accorde ensuite un périmètre décisionnel précis, qui est qualifié dans cet exemple par la libre disposition de son corps.

66. Mais si cette approche parait novatrice dans sa forme, elle s'appuie en réalité sur des éléments déjà identifiés par la jurisprudence et la doctrine. Pris dans leur ensemble, ces éléments suggèrent que le droit au respect de la vie privée est bien tel que nous le concevons, c'est à dire avant tout une protection de la faculté d'autonomisation (Section 1) auquel est associé un périmètre décisionnel individuel et objectif (Section 2)

Section 1

La protection de la faculté d'autonomisation

67. Si le droit au respect de la vie privée est, dans un premier temps, une protection de la faculté d'autonomisation, il doit nécessairement garantir l'aptitude à posséder une singularité dans un groupe social donné. Pour cela, il est important que l'agent[151] soit dans un environnement structurel permettant l'éclosion de cette pensée individuelle, non pas en observant cette capacité d'autonomie à un instant donné, mais bien en analysant le cheminement qui peut conduire l'individu à un tel état. En effet, cette structure est d'abord mentale avant d'être physique, comme le confirme de nombreuses études sociales et philosophiques mettant en avant la nécessité d'un isolement de la pensé vis-à-vis des immixtions externes en amont de toute situation de décision.

150 CEDH, gr. ch., 11 juillet 2002, *Christine Goodwin c. Royaume-Uni*, n°28957/95, para. 90.

151 Dans l'ensemble de notre réflexion, nous prendrons comme base de la définition « *d'agent* » le sens donné par le courant dit « *objectiviste* » initié par Durkheim et dont Bourdieu développe l'idée. Ainsi, l'agent est un individu sensible à son milieu, milieu qui exerce sur lui une pression indirecte quant à son comportement en définissant l'*habitus*. L'agent est toujours libre de ses choix, cependant, il est possible de prédire dans une certaine mesure ses décisions en analysant la structure sociale dans laquelle il évolue, ou tout du moins, de définir un model statistique qui va suggérer la tendance comportementale pour les agents d'un même milieu. v. Bourdieu Pierre, *Le Sens Pratique*, Les Editions de Minuit, 1 février 1980, 500 p.; Durkheim Emile, *Les Règles de la Méthode Sociologique*, Flammarion, 10 Mars 2010, 333 p.

68. Selon Montaigne, « *il faut se réserver une arrière-boutique toute notre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude* » [152]. Par cette maxime, il révèle une distinction sémantique fondamentale entre une « *liberté* » sociale qui serait contraignante et une « *vraie liberté* » qui s'exercerait uniquement dans la solitude. Cette liberté serait différente de ce que certains identifient comme la liberté physique[153], pour se confondre avec les notions voisines de liberté morale et de liberté intellectuelle[154]. Pour le philosophe fortement marqué par les guerres de religions, cet idéal semble se rapprocher par l'esprit de ce que Schopenhauer désignera par la suite comme le « *liberum arbitrium indifferentiae* » ou « *liberté d'indifférence* »[155], qui serait la théorie d'une liberté absolue à laquelle un homme n'accède qu'en l'absence de motifs ou de raisons externes. Une sorte de liberté pure dans laquelle la volonté peut se forger.

69. Pour Hannah Arendt, cet isolement permet de faire éclore une morale qui « *concerne l'individu dans sa singularité* »[156] grâce à un dialogue intérieur avec lui-même. Une sorte de maïeutique par laquelle l'individu décide pour lui en toute indépendance. C'est d'ailleurs cette intégrité et les risques qu'entraîne un contrôle social de celle-ci qui est mis en avant dans l'étude de Michel Terestchenko sur les atrocités de la seconde guerre mondiale[157]. Il s'attarde particulièrement sur des cas documentés de résistances et d'actions de personnes ayant agi contre le courant historique, en dépit de leur intérêt personnel et malgré les risques encourus. Pour ces personnes, il apparaît que c'est cette capacité de repli intérieur, d'appel au « *for intérieur* » qui a été la base de leur action. Cette expression prémonitoire des conclusions d'Arendt, trouve son origine sémantique dans le mot For, qui désignait autrefois un tribunal de justice, lui-même provenant du « *forum* » latin[158]. Ce lieu intérieur est donc la place du dialogue intime par lequel un individu peut forger sa décision. C'est d'ailleurs une notion

152 Montaigne Michel (de), *Les Essais*, PUF, 9 juillet 2004, p. 345.

153 « *La liberté physique consiste dans l'absence d'obstacles matériels de toute nature. […] Mais le plus souvent, dans notre pensée, l'idée de la liberté est l'attribut des êtres du règne animal, dont le caractère particulier est que leurs mouvements émanent de leurs volontés, qu'ils sont, comme on dit, volontaires, et on les appelle libres lorsqu'aucun obstacle matériel ne s'oppose à leur accomplissement* ». Schopenhauer Arthur, *Essai sur le Libre Arbitre*, Rivages, 2 mars 1992, p. 7.

154 Ibid. pp. 9-13.

155 Ibid, p. 17.

156 Arendt Hannah *Responsabilité et Jugement*, Payot, 5 mars 2009, 362 p.

157 Terestchenko Michel, *Un si Fragile Vernis d'Humanité*, La Découverte, 4 octobre 2007, 308 p.

158 Bonnaventure de Roquefort Jean Baptiste, *Dictionnaire Etymologique de la Langue Françoise*, Volume 1, Décourchant, 1829, p. 332.

connexe de la délibération Aristotélicienne, dans laquelle l'agent effectue ce même dialogue intérieur[159]. Enfin pour Stuart Mill, c'est « *le domaine intime de la conscience qui nécessite la liberté de conscience au sens le plus large : liberté de penser et de sentir, liberté absolue d'opinions et de sentiments sur tous les sujets, pratiques ou spéculatifs, scientifiques, moraux ou théologiques* » [160].

70. À première vue sur le plan juridique, cette capacité de décision se rapproche du droit à la libre pensée. L'article 18 de la déclaration universelle des droits de l'homme énonce : « *toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté de changer de religion ou de conviction ainsi que la liberté de manifester sa religion ou sa conviction seule ou en commun, tant en public qu'en privé, par l'enseignement, les pratiques, le culte et l'accomplissement des rites* » [161]. La Cour Européenne des Droits de l'Homme a d'ailleurs rappelé que ce bastion intérieur de la pensée humaine est « *un droit absolu et ne peut faire l'objet d'aucune restriction* »[162]. Ce n'est donc qu'avec réticence que celle-ci observe les affaires y ayant trait, notamment lorsqu'elle commence son observation par : « *bien que l'idée d'une décision de justice rendue par l'Etat sur la nature des convictions intimes et personnelles d'un citoyen fasse horreur et puisse avoir un relent malheureux des infâmes persécutions d'autrefois, la Cour observe […]»*[163].

71. Pourtant, nous n'abordons qu'en partie la protection accordée par l'article 9, de la Convention de sauvegarde des Droits de l'Homme et des libertés Fondamentale[164], qui prône

159 Au sens de la *bouleusis* Aristotélicienne : « *Mais nous délibérons sur les choses qui dépendent de nous et que nous pouvons réaliser : et ces choses-là sont, en fait, tout ce qui reste, car on met communément au rang des causes, nature, nécessité et fortune, et on y ajoute l'intellect et toute action dépendant de l'homme. Et chaque classe d'Homme délibère sur les choses qu'ils peuvent réaliser par eux-mêmes* ». Aristote, *Ethique à Nicomaque*, Vrin, 1 janvier 1994, p. 63-64.

160 Mill John Stuart, *De la Liberté*, Jean-Marie Tremblay, 19 mai 2002, p. 13.

161 Déclaration Universelle des Droits de l'Homme, texte adopté le 10 décembre 1948 par l'Assemblée Générale des Nations Unies, article 18.

162 En faisant référence aux conclusions de l'affaire *Buscari et autres c. Saint Martin du 4 mai 200*, Comité Directeur pour les Droits de l'Homme, Groupe de rédaction sur les droits de l'homme dans les sociétés culturellement diverses, *Déclarations publiques lors du Projet de Compilation des normes du Conseil de l'Europe relatives aux principes de liberté de pensée, de conscience et de religion et liens avec d'autres droits de l'homme*, Conseil de l'Europe, Strasbourg, 11 Mars 2015, Point 24.

163 « *While the notion of the State sitting in judgment on the state of a citizen's inner and personal beliefs is abhorrent and may smack unhappily of past infamous persecutions, the Court observes that …»* CEDH, 13 avril 2006, *Koteski c. République Yougoslave de Macédoine*, n°39630/09.

164 « *Article 9 – Liberté de pensée, de conscience et de religion : 1 – Toute personne a droit à la liberté de pensée, de conscience et de religion ; ce droit implique la liberté de changer de religion ou de conviction, ainsi que la liberté de manifester sa religion ou sa conviction individuellement ou collectivement, en public ou en privée, par le culte, l'enseignement, les pratiques et l'accomplissement des rites. 2 – La liberté de*

la liberté de pensée, de conscience et de religion. Il ne s'agit pas de manifester sa religion ou sa pensée, mais bien de la concevoir en son for intérieur. Or si l'article 9 consacre une protection de la pensée, celle-ci doit nécessairement s'appuyer sur la capacité d'un individu à s'isoler intérieurement pour la forger, sans être l'objet d'une interaction externe.

72. Confirmant ce point, la Cour Européenne des Droits de l'Homme énonce que « *la notion de vie privée englobe l'intégrité physique et morale de la personne* » [165]. Selon ces réflexions, cet état théorique ne pourrait exister que si le sujet se place dans une situation où il n'est pas soumis à une interférence extérieure qui limiterait sa propre réflexion par une quelconque influence[166]. Il s'agit d'un espace essentiel de développement personnel, que la jurisprudence Européenne associe à la notion de vie privée[167], dans lequel l'individu peut se forger sa propre grille morale qui lui permettra ensuite d'agir selon sa volonté dans la société. En se plaçant sur ce terrain, le droit au respect de la vie privée devient le défenseur d'une liberté de pensée et des prémices de la décision d'agir en accord avec celle-ci. Il devient même la condition sine qua non de la capacité des êtres à se constituer de façon singulière, en suivant ce que la jurisprudence désigne par « *le for intérieur* » [168].

73. C'est donc un point charnière entre la vie privée et la liberté de pensée qu'il convient de définir, notamment au regard des progrès technologiques relatifs à la lecture des pensées[169]. En effet, certaines études informatiques s'orientent vers la détection des émotions dans l'expression humaine avec un simple appareil utilisé pour les jeux vidéo[170]. Il s'agit là de technologies balbutiantes, mais qui risquent d'avoir une évolution rapide dans les années

manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publiques, ou à la protection des droits et libertés d'autrui ». Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales telle qu'amendée par les Protocoles n°11 et n°14, Rome, 4 novembre 1950.

165 CEDH, 25 mars 1993, *Costello-Roberts c. Royaume-Uni*, n°13134/87, considérant 34.

166 On peut ici rapprocher ces réflexions des écrits d'Aristote sur l'activité volontaire et la contrainte comme motivation de l'action des hommes, qui considère qu'un acte forcé est « *tout ce qui a son principe hors de nous*». Ainsi, s'il existe un motif extérieur, l'action n'est pas totalement volontaire. v. Aristote, *Ethique à Nicomaque*, Vrin, 1 janvier 1994, p.58.

167 CEDH, gr. ch., 11 juillet 2002, *Christine Goodwin c. Royaume-Uni*, n°28957/95, para. 90.

168 « *La Commission rappelle que l'article 9 protège avant tout le domaine des convictions personnelles et des croyances religieuse, c'est-à-dire celui que l'on appelle parfois le for intérieur* ». CEDH, 22 février 1995, *Van Den Dungen c. Pays-Bas*, n°22838/93.

169 Sender Elena, *Lire dans les Pensées ? Les Neurosciences Y Sont Presque*, Sciences et Avenir, 19 juin 2015, disponible sur https://www.sciencesetavenir.fr/sante/lire-dans-les-pensees-les-neurosciences-y-sont-presque_29175 (consulté le 01/02/17).

170 Mao Qi-rong, Pan Xin-yu, Zhan Yong-zhao, Shen Xian-jun, *Using Kinect for real-time emotion recognition via facial expressions*, Frontiers of Information Technology & Engineering, 2015 16(6), pp. 272-282.

futures. À la lumière de ces nouvelles atteintes potentielles, il convient de souligner l'importance du droit au respect de la vie privée pour l'individu, en s'attachant à définir la protection qu'il érige autour de la capacité d'autonomisation.

1 – L'identification des structures affectant la capacité décisionnelle

74. En l'absence d'élément coercitif identifié, il est difficile de qualifier juridiquement l'action que peut avoir une personne extérieure sur la capacité d'un individu à prendre une décision librement.

75. L'une des solutions est le recours à la notion de liberté dans le consentement. En prenant l'exemple du consentement à la mise en ligne d'une photographie de l'employé sur le site internet de l'entreprise, le Groupe de travail sur l'article 29 relève que « *le travailleur peut en théorie, refuser de donner son consentement, mais il peut perdre alors une opportunité d'emploi. Dans ces circonstances, le consentement n'étant pas donné librement, n'est donc pas valable* » [171]. Mais si l'on se réfère à cette conception, il faut nécessairement prouver l'existence tangible d'un élément coercitif. En l'espèce, la possibilité de ne pas être recruté.

76. La notion de violence procède de la même logique. Inscrite dès 1804 dans le code civil, elle prohibe toute action *« de nature à faire impression sur une personne raisonnable [pouvant] lui inspirer la crainte d'exposer sa personne ou sa fortune à un mal considérable et présent* » [172]. De plus, la violence doit être illégitime pour être retenue par les tribunaux[173] malgré la prise en compte avec parcimonie de l'exploitation des circonstances dans certains cas d'espèces où la menace est particulièrement ressentie. Par exemple, lors de l'occupation d'un navire[174], ou lors d'un accord passé dans des conditions d'agitations sérieuses[175].

---

171 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 5.

172 Code Civil, article 1112, Créé par la loi 1804-02-07 promulguée le 17 février 1804 : « *Il y'a violence lorsqu'elle est de nature à faire impression sur une personne raisonnable et qu'elle peut lui inspirer la crainte d'exposer sa personne ou sa fortune à un mal considérable et présent. On a égard, en cette matière, à l'âge, au sexe et à la condition des personnes ».*

173 Cass. Com., 20 mai 1980, n°78-10833, Bull. Com. IV, n°212.

174 Cass. Soc., 8 novembre 1984, n°82-14816, Bull. Soc. 1984, V, n°423.

175 T. civ. Nantes, 6 janv. 1956, Gaz. Pal. 1956, 1, 61.

77. Pourtant, il peut exister des structures à l'intérieur desquelles l'individu est affecté dans sa capacité décisionnelle, sans élément coercitif identifié, et pour lesquelles notre définition de la vie privée, en tant que protection de la capacité d'autonomisation et du périmètre décisionnel, prend tout son sens. Pour comprendre ce processus, nous prendrons comme exemple le Panoptique[176], conceptualisé par Jeremy Bentham[177] et analysé par Foucault[178]. Celui-ci correspond à une structure carcérale circulaire, à l'intérieure de laquelle les détenus sont placés en périphérie de l'anneau. Le surveillant se place au centre de l'architecture, et bénéficie d'un point de vue englobant la totalité des cellules. Par l'effet optique obtenu par l'agencement des ouvertures extérieures, les détenus sont toujours visibles grâce au contre-jour qui traverse leur cellule de part en part. Pour autant, ceux-ci ne peuvent voir l'observateur central qui se situe, lui, dans l'ombre. Un peu comme des ombres chinoises, le surveillant sera en mesure de contrôler l'activité de chacun des détenus, sans pour autant que ceux-ci puisse en discerner l'activité.

78. L'individu devient selon Foucault « *l'objet d'une information, jamais sujet dans une communication* »[179]. Un des premiers effets est alors la capacité d'individualiser la surveillance. Au lieu de se situer au milieu d'un groupe d'individus difficilement différentiables, le détenu est seul dans une unité qui lui est affecté. Par corollaire, il sera responsable de sa propre conduite. Dès lors, « *celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir ; il les fait jouer spontanément sur lui-même ; il inscrit en soi le rapport de pouvoir dans lequel il joue simultanément les deux rôles ; il devient le principe de son propre assujettissement* » [180].

79. Dans cette configuration, il est difficile d'affirmer que la liberté de penser fait l'objet d'une réelle limitation alors qu'elle peut subsister dans le for intérieur du condamné. Mais il serait dommageable de ne pas prendre en compte l'effet psychologique d'une telle surveillance. De fait : « *un assujettissement réel nait mécaniquement d'une relation fictive. De*

176 Le terme Panoptique est l'association du grec παν (ensemble, tout) et de οπτικος (optique, observer), décrivant ainsi l'objectif poursuivi par la structure architecturale.
177 v. Trotignon Pierre, *BENTHAM JEREMY - (1748-1832),* Encyclopædia Universalis, disponible sur http://www.universalis.fr/encyclopedie/jeremy-bentham/ (consulté le 01/07/17).
178 Foucault Michel, *Surveiller et Punir,* Gallimard, 20 février 1975, 352 p.
179 Ibid, p. 202.
180 Ibid, p. 204.

sorte qu'il n'est pas nécessaire d'avoir recours à des moyens de force pour contraindre le condamné à la bonne cuite, le fou au calme, l'ouvrier au travail, l'écolier à l'application, le malade à l'observation des ordinaires » [181]. On se trouve alors dans un mécanisme de conditionnement indirect du comportement humain, sans élément coercitif identifié.

80. Si l'on se réfère à la définition du droit au respect de la vie privée telle que la doctrine la propose, sous la forme d'une sphère d'intimité, cette surveillance constitue bien une immixtion, mais reste acceptable au regard de la nécessité de surveiller le détenu[182]. Pourtant, cet exemple met en évidence l'influence de la structure carcérale sur la capacité décisionnelle de l'individu. En introduisant une surveillance, on est capable de normaliser les comportements. Si celle-ci est acceptable pour un détenu, l'est-elle à l'échelle d'une société ? À cela, la définition doctrinale peine à répondre, puisqu'elle s'appuie avant tout sur l'analyse de la proportionnalité de la mesure par rapport au but recherché. Ainsi, le déploiement d'une vidéoprotection nationale est justifié pour des raisons de sécurité[183]. La vidéo-surveillance constante est légitime pour les personnes « *dont l'évasion ou le suicide pourraient avoir un impact important sur l'ordre public eut égard aux circonstances particulières à l'origine de leur incarcération et l'impact de celles-ci sur l'opinion publique* » [184]. De la même manière, la récente loi sur le renseignement autorise des captations de données extrêmement étendues au nom de la sécurité nationale[185].

81. Cela révèle une faiblesse dans l'approche classique de la définition du concept de vie privée. Dans chaque cas, la définition doctrinale ne peut que constater une atteinte, sans analyser son impact plus profond sur l'individu alors qu'elle l'excuse dans le même temps au regard de la proportionnalité de la mesure. Cette structure juridique génère une faculté d'autojustification de n'importe quelle mesure attentatoire. Ainsi, la récente loi relative au renseignement autorise la mise en place de ce que l'on peut qualifier de « *boites noires* » dans les principaux services informatiques (fournisseurs d'accès ou de services) capables

181 Ibid, p. 204.

182 v. Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales telle qu'amendée par les Protocoles n°11 et n°14, Rome, 4 novembre 1950, article 8-2.

183 Loi n° 2011-267 du 14 mars 2011, *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n°0062 du 15 mars 2011, p. 4582, texte n°2.

184 Commission Nationale de l'Informatique et des Libertés, *Vidéo dans les cellules de détention : l'avis de la CNIL*, 14 juin 2016, disponible sur https://www.cnil.fr/fr/video-dans-les-cellules-de-detention-lavis-de-la-cnil (consulté le 01/09/17).

185 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

d'intercepter l'ensemble des informations y transitant. Selon celle-ci : « *dans les conditions prévues […] et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction des paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste* » [186]. De fait, la surveillance quasi complète du réseau internet Français se trouve justifiée par la menace terroriste sans que la question de l'impact sur la vie privée ne puisse être soulevée. En suivant cette logique, on peut imaginer n'importe quelle mesure attentatoire à la vie privée jugée légitime au nom de l'objectif qui lui convient. Si l'on ne peut, d'un point de vue scientifique, juger de la pertinence de ces mesures, on peut critiquer la logique juridique qui réduit considérablement la portée de l'analyse que l'on peut faire de l'atteinte au droit au respect de la vie privée. Dans un contexte de menace terroriste persistante, l'approche classique ne peut constituer un rempart suffisant à l'appétit des Etats. Enfin, la définition classique ne peut rendre compte des conséquences de la mise en présence d'un individu avec un autre. Une personne n'aura pas forcément le même comportement lorsqu'elle est seule ou lors de la présence de son conjoint.

82. À l'inverse, en prenant la première partie de notre définition du droit au respect de la vie privée, comme une protection de la faculté d'autonomisation, nous sommes capables non seulement de constater l'existence d'une telle surveillance, mais encore d'en qualifier l'impact sur la personne. La question de la proportionnalité d'une mesure législative ne se fait plus en comparant les objectifs et les moyens, mais la mesure dans son ensemble face à la réduction potentielle de la capacité décisionnelle des personnes, que celle-ci soit auto-infligée ou résultant d'un élément coercitif latent. En cela, on peut s'appuyer sur la notion doctrinale de liberté personnelle pour définir une structure d'analyse juridique.

186 Ibid.

2 – Une protection de la liberté personnelle

83. La liberté personnelle est une notion quasiment absente du droit Français. Aucun texte n'y fait explicitement référence alors que la jurisprudence l'utilise ponctuellement pour qualifier certaines atteintes à la sensibilité psychologique des individus. Elle est un moyen d'étendre la protection des personnes qui, placées dans une certaine structure, pourraient être limitées indirectement dans l'utilisation de leur liberté individuelle. Ce n'est pas l'absence de procédure permettant l'exercice d'une liberté qui est jugée, mais si la personne est en pleine capacité de l'exercer. En cela, nous reprenons la distinction sémantique doctrinale qui définit la liberté personnelle comme « *le droit à ne pas subir de contraintes excessives*»[187] et qui, selon Henry Roussillon et Xavier Bioy, relève de la liberté de l'individu d'une façon distincte de la liberté individuelle[188].

84. La notion s'oppose à la réduction doctrinale systématique de la vie privée à sa relation aux libertés individuelles. Ainsi, dans sa décision du 18 Janvier 1995 portant sur la loi d'orientation et de programmation relative à la sécurité, le Conseil Constitutionnel déclarait que *« la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* »[189]. La décision suggère que la privation d'une liberté individuelle constitue un dommage pour le citoyen. Mais elle ne pose pas la question de savoir si le déploiement d'une technologie de surveillance peut indirectement le priver d'exercer une liberté, par sa simple présence. La même logique est d'ailleurs reprise par la CNIL lorsqu'elle analyse une mesure, puisqu'elle s'appuie sur de « *forts enjeux, tant en matière de respect des libertés individuelles que du cadre juridique dans lequel ils doivent s'inscrire* »[190]. Selon cette approche, l'analyse se borne à savoir si une liberté individuelle est, de fait, impossible à exercer par le citoyen à cause, par exemple, d'une mesure touchant à sa vie privée dans le cadre de la privation de sa liberté de circuler. Ce raisonnement réduit donc la portée du concept de vie privée à sa portion congrue.

187 Mathieu Bertrand, *Droit Constitutionnel Civil*, Jurisclasseur Administratif, 1997, Fasc. 1449, 1990, p. 15.
188 v. Roussillon Henry, *Liberté Personnelle: une Autre Conception de la Liberté ?*, Presses de l'Université des Sciences Sociales de Toulouse, 1 juin 2006, 159 p.
189 Conseil Constitutionnel, Décision N° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 - Journal officiel du 21 janvier 1995, p. 1154, considérant 3.
190 Commission Nationale de l'Informatique et des Libertés, *Vidéo dans les cellules de détention : l'avis de la CNIL*, 14 juin 2016, disponible sur https://www.cnil.fr/fr/video-dans-les-cellules-de-detention-lavis-de-la-cnil (consulté le 01/09/17).

85. À l'inverse, la notion de liberté personnelle correspond à la reconnaissance juridique d'une sensibilité d'ordre psychologique des individus vis-à-vis de leur environnement social, et constitue une protection face à une influence structurelle qui serait néfaste à l'individu. Dans la décision du 20 juillet 1988, le Conseil Constitutionnel reconnaissait que la réintégration d'un salarié amnistié de ses violences passées pouvait « *affecter la liberté personnelle de l'employeur et de ses salariés de l'entreprises en leur imposant la fréquentation, sur les lieux de travail, des auteurs d'actes dont ils ont été victimes* » [191]. Dans l'absolu, la réintégration d'une personne ne va pas venir diminuer la capacité de l'employeur ou de ses salariés à exercer leurs libertés individuelles. Mais cela va constituer un facteur de limitation de leur expressivité, prenant dès lors une connotation psychosociologique. Cette présence non désirée, mais statutairement validée, va venir exercer une contrainte indirecte sur les salariés anciennement victimes de l'action fautive, par un phénomène d'autocensure de leurs comportements respectifs.

86. Or, pour le Conseil Constitutionnel, une telle situation est contraire au respect des articles 2 et 4 de la déclaration des Droits de l'Homme et du Citoyen de 1789 concernant le respect de la liberté et de l'exercice des droits naturels, auquel il rattache la liberté personnelle dans sa décision datée du 20 novembre 2003[192]. En l'espèce, le considérant 94 fait une application concrète de cette analyse. Il s'agissait de savoir si le caractère irrégulier du séjour d'un étranger pouvait constituer, par lui-même, un obstacle au mariage. La capacité de choisir son partenaire marital, caractérisée par la liberté du mariage, va devenir une « *composante de la liberté personnelle* » [193]. L'obstacle juridique va donc être jugé contraire à la liberté personnelle, en la distinguant très finement de la liberté individuelle. Il est en effet possible de limiter la liberté du mariage, en cas notamment d'absence réelle d'intention matrimoniale[194], donc de limiter la liberté individuelle de se marier, mais pas de limiter la liberté personnelle de choisir son partenaire en amont de ce contrôle. En conséquence, le

191 Conseil Constitutionnel, Décision n° 88-244 DC du 20 juillet 1988, *Loi portant amnistie*, Rec. p. 119 - Journal officiel du 21 juillet 1988, p. 9448, considérant 44.

192 Conseil Constitutionnel, Décision n° 2003-484 DC du 20 novembre 2003, *Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité*, Rec. p. 438 - Journal officiel du 27 novembre 2003, p. 20154.

193 Ibid, considérant 94.

194 Loi n° 93-1417 du 30 décembre 1993 portant diverses dispositions relatives à la maitrise de l'immigration et modifiant le code civil.

Conseil Constitutionnel considère que le caractère irrégulier du séjour d'un étranger ne peut faire obstacle, en soit, au mariage de l'intéressé.

87. Dans cette décision, le Conseil Constitutionnel considère que cette mesure pourrait « *dissuader les intéressés de se marier ; qu'ainsi, elles portent également atteinte au principe constitutionnel de la liberté du mariage* » [195] et donc, à la liberté personnelle. C'est une véritable reconnaissance de la liberté personnelle qui est faite au niveau constitutionnel. Non seulement celle-ci devient une notion reconnue, mais elle est également une composante de nombreuses autres libertés. Dans l'affaire précédente, par syllogisme, l'individu était influençable dans le choix de son partenaire, la liberté personnelle n'était pas respectée (dissuasion), donc la liberté du mariage n'était pas respectée. Ce faisant, la notion de liberté personnelle devient un outil n'analyse de la possibilité d'exercer une liberté donnée. Si la liberté personnelle est respectée, cela veut dire que le cadre dans lequel la personne se trouve est favorable à l'exercice de ses autres libertés.

3 – Un sanctuaire de la capacité décisionnelle des personnes

88. La notion de liberté personnelle est donc un moyen d'analyser une structure sociale ou juridique dans laquelle évolue un individu, afin de savoir si celui-ci conserve la liberté d'exercer les choix que sa conscience lui dicte. S'il ne subit pas de pressions externes, sa liberté personnelle est respectée et il est en mesure d'exercer ses libertés individuelles. À l'inverse, toute restriction de sa liberté personnelle impacte l'exercice de ses libertés individuelles. Nous pouvons arriver à la même conclusion en suivant un raisonnement systématique, en se plaçant cette fois du point de vue de l'utilisation finale d'une liberté individuelle et en observant si la structure lui permet de l'exercer sans contrainte. Or cette structure correspond à la première partie de notre définition du droit au respect de la vie privée, en tant que faculté d'autonomisation des personnes.

195 Conseil Constitutionnel, Décision n° 2003-484 DC du 20 novembre 2003, *Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité*, Rec. p. 438 - Journal officiel du 27 novembre 2003, p. 20154, considérant 96.

89. Dans sa décision datée du 15 décembre 1983[196], la Cour Constitutionnelle Allemande utilise ainsi, pour juger de la légalité d'un fichier de traitement de données au regard de la vie privée, la possibilité que celui-ci nuise aux droits de la personne définie par l'article 1er de la Constitution Allemande sur la dignité de l'être humain[197], ainsi que l'article 2 directement lié au « *développement personnel* »[198]. Pour celle-ci, « *l'autodétermination individuelle présuppose que l'individu continue à disposer de sa liberté de décider d'agir ou de s'abstenir, et de la possibilité de suivre cette décision en pratique. Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celle-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée* » [199] . La notion de liberté personnelle reconnait donc, en corollaire, un effet sur le développement de la personnalité humaine, ou tout du moins, sur la capacité d'épanouissement à long terme d'une personne dans un environnement social donné. Elle vient ainsi se distinguer de l'utilisation de la liberté individuelle de l'article 66 de la Constitution[200] pour y adjoindre un « *proche parent du libre développement de la personnalité* » [201] qui se rattache aux articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen[202]. Par conséquent, il serait inopportun de suivre la doctrine considérant le droit au respect de la vie privée sous l'angle unique de l'exercice des libertés individuelles, alors même que celles-ci dépendent de la liberté personnelle.

90. Plus encore, dans l'affaire Ammann/Suisse du 16 févier 2000, la Cour Européenne des droits de l'homme précise que *« le terme « vie privée » ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour un individu de nouer et développer des relations avec ses semblables »* [203]. Ce droit n'est donc pas

196 Bundes VerfassungsGericht. Volkszahlungsurteil, BVEerfGE Bd. 65, S. 1 FF, 15 Décembre 1983.

197 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 23. Dezember 2014 (BGBl. I S. 2438) geändert worden ist, Article 1.

198 *« Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt ».* Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 23. Dezember 2014 (BGBl. I S. 2438) geändert worden ist, Article 2.

199 Bundes VerfassungsGericht. Volkszahlungsurteil, BVEerfGE Bd. 65, S. 1 FF, 15 Décembre 1983, p26.

200 Constitution du 4 octobre 1958, article 66.

201 Bioy Xavier. *Le Libre Développement de la Personnalité en Droit Constitutionnel Essai de Comparaison (Allemagne, Espagne, France, Italie, Suisse),* Revue internationale de droit comparé. Vol. 55 N°1. Janvier-mars 2003, p. 133.

202 Déclaration des droits de l'homme et du citoyen de 1789, article 2 et 4.

203 CEDH, gr. ch., 16 février 2000, *Amann c. Suisse*, n° 27798/95, considérant 65.

seulement une protection de la liberté individuelle, dont l'article 66 de la Constitution ordonne à l'autorité judiciaire d'assurer la protection et n'intégrant pas le droit de nouer des relations amicales, mais il concerne également la liberté personnelle qui peut être rattachée à cette dimension sociale. Par conséquent, avant même de parler de la capacité d'exercer certains droits, il faut reconnaître à l'individu un droit à vivre dans une structure permettant la conception de ces derniers. À l'intérieur de celle-ci, le droit au respect de la vie privée apparait comme un élément fondamental, capable de garantir à l'individu sa capacité de développement et à forger sa propre conception de l'exercice de ses libertés.

91. Le droit au respect de la vie privée doit donc être conçu, au moins en partie, comme une protection de la faculté d'autonomisation des personnes, véritable sanctuaire nécessaire à l'exercice de la liberté personnelle et des libertés individuelles.

Conclusion

92. L'idée d'une société de surveillance totale a été portée à l'extrême dans une ville fictive imaginée par Alain Damasio, Cerclon, dans son roman la Zone du Dehors[204]. Dans celle-ci, un système panoptique est installé au centre de chaque quartier, épiant les moindres faits et gestes des citoyens, et où chaque entrée de bâtiment, de rue, est soumise à un contrôle informatisé. Le simple fait d'entrer dans un magasin nécessite une vérification de la présence sur le compte en banque d'une somme suffisante pour faire un achat. Nous sommes dans une rationalisation extrême du comportement humain, voire d'un utilitarisme Benthamien[205] poussé jusqu'à la caricature.

204 Dans son livre, Arendt Hannah, *Condition de l'Homme Moderne*, Pocket, 28 Août 2002, 416 p., Hannah Arendt développe l'idée, dans sa description de la *vita activa*, que l'action (politique) de l'homme est forcément concurrente de son interaction sociale. Elle fait ainsi une opposition entre l'activité de travail qui peut s'effectuer seul, et celle politique qui doit nécessairement s'appuyer sur un relai social pour exister. Elle relève ainsi la difficulté soulevée par le concept de domaine social, auquel les catégories de privé et de public s'appliquent difficilement puisqu'elles s'y retrouvent mêlées, justifiant ainsi son recours à des néologismes.

205 Dans son livre, An introduction to the Principles of Morals and Legislation de 1781, Betham prône une définition de l'utilitarisme dont l'objectif serait l'idée que toute action doit être évaluée selon sa tendance à engendrer le bien être du plus grand nombre. Ainsi, « *it has been shown that the happiness of individuals, of whom a community is composed, that is their pleasures and their security, is the end and the sole end which the legislator ought to have in view : the sole standard, in conformity to which each individual ought, as far as depends upon the legislator, to be made to fashion his behavior*", Bentham Jeremy, *An introduction to The Principles of Morals and Legislation*, Courier Corporation, 7 mars 2012, p. 27. Dans cette structure, Bentham

93. Cela va plus loin que le célèbre Big Brother imaginé par Orwell[206]. Dans ce dernier, c'est le pouvoir en place qui gardait le pouvoir principal de coercition des actions contraires à son ordre établi. À l'inverse dans notre exemple, les citoyens ont accepté de faire partie de cette société qui les protège. C'est le passage de la société de discipline à la société de contrôle selon Deleuze : « *ce sont les sociétés de contrôle qui sont en train de remplacer les sociétés disciplinaires. Contrôle, c'est le nom que Burroughts propose pour désigner le nouveau monstre, et que Foucault reconnait comme notre proche avenir* »[207]. Plus poétiquement, Damasio le qualifie de « *Big Mother* »[208]. La nuance se tient donc dans l'acceptation de cette surveillance de fait, et sur l'acceptation de sa destination. De plus, si on laisse se développer ce « *monstre doux* »[209], selon l'appellation de Jean-Jacques Lavenue, le citoyen sera-t-il capable de retrouver un niveau de protection suffisant ? Alors que l'ancien ministre de l'intérieur, Bernard Cazeneuve, considérait en 2015 que la vie privée n'était qu'un droit n'ayant pas de lien avec les libertés individuelles[210], il parait important de conserver ces prédictions à l'esprit.

---

affirme que les intérêts collectifs et individuels sont identiques, et par conséquent, consubstantiels. Cependant, en faisant ce postulat, l'auteur n'analyse l'action que sur le fondement du bonheur global escompté et non sur la morale. Dès lors, la justification d'une action contraire à un individu particulier peut être validée par une théorie utilitariste malgré sa moralité discutable. On peut aisément penser aux pratiques eugénistes dont l'objectif affiché est l'amélioration du patrimoine génétique d'une population qui peuvent prendre des formes moralement inacceptables.

206 Orwell George, *1984*, Gallimard, 16 décembre 1972, 438 p.

207 Deleuze Gilles, *Post-Scriptum sur les sociétés de Contrôle*, Publié dans Pourparlers, Les Editions de Minuit, Paris, 1990, pp. 240-247.

208 « *C'est une réaction à la fois hyper stupide et hyper soumise. La personne qui dit ça a déjà endogénéisé le contrôle : « Allez-y, je suis transparente, transpercez-moi avec la lumière et au moins, on verra ceux qui sont un peu trop opaques ! ». Je trouve ce discours de servitude volontaire dramatique, dangereux et grave politique. Avec les outils qu'on a aujourd'hui, si on était dans les conditions politiques de la Deuxième guerre mondiale, on se ferait laminer par la machine ! On est en train de potentialiser un abus planétaire de pouvoir. Et j'ai vraiment l'impression qu'il y a eu un basculement. La sécurité est devenue un affect plus enviable que la liberté. C'est pas Big Brother, c'est Big Mother ! C'est un pouvoir disciplinaire, c'est la mère couvrante qui nous enveloppe ! Des gens sont rassurés par une caméra de surveillance !* ». Damasio Alain, Propos recueillies dans : Fradin Andréa, *L'auteur de SF Alain Damasio dissèque la société de contrôle « C'est pas Big Brother c'est Big Mother »*, Les Inrocks, 25 novembre 2013, disponible sur http://www.lesinrocks.com/2013/11/25/medias/lauteur-sf-alain-damasio-disseque-societe-controle-cest-pas-big-brother-cest-big-mother-11447605/ (consulté le 01/09/2017).

209 v. Lavenue Jean-Jacques, *Gouvernance des données et naissance du Monstre Doux,* in Bouhadana Irene, Gilles William, *Droit et gouvernance des données publiques et privées à l'ère du numérique,* Imodev, 2015, pp. 35-56.

210 « *Il n'y a, dans ce texte de loi, aucune-je dis bien : aucune – disposition attentatoire aux libertés, qu'il s'agisse de la liberté d'aller et venir ou d'autres libertés individuelles ou collectives. Si vous estimez qu'un article de ce texte est susceptible de remettre en cause une liberté, des moi lequel. En revanche, il est des dispositions qui peuvent être considérées comme remettant en cause la vie privée et le droit à cette dernière* ». Cazeneuve Bernard, *Déclaration publique lors du compte rendu intégral de la Première séance du Mardi 14 Avril 2015*, Assemblée Nationale, 14 avril 2015.

94. Car ces déploiements relèvent de la conception même de la notion de vie privée. Si l'on considère la définition doctrinale classique, ainsi que l'analyse d'acceptabilité juridique basée sur la proportionnalité des mesures, ces systèmes ne sont pas illicites au regard du droit au respect de la vie privée. Pourtant, en partant de la reconnaissance de l'influence qu'exerce le milieu sur l'individu, on peut concevoir le droit au respect de la vie privée comme une structure de protection érigée autour de la capacité d'autonomisation décisionnelle des individus. L'analyse juridique de la proportionnalité d'une mesure législative bascule alors de son objectif face celle-ci, à la mesure contre son impact réel. Il s'agira donc de savoir si la liberté personnelle est suffisante pour permettre l'exercice des libertés individuelles. La combinaison des notions de liberté personnelle et de liberté individuelle, toutes deux reconnues au niveau constitutionnel, devient alors une boussole permettant de qualifier l'impact d'une mesure sur l'individu.

95. Toutefois, cette approche comporte certains défauts. Premièrement, on peut reconnaître le fait qu'en s'inscrivant dans un environnement matériel, il existera toujours une contrainte indirecte qui sera applicable à l'agent. Si la simple présence d'une personne peut influencer la décision d'exercer une action, la possibilité qu'une action réalisée par une personne seule soit diffusée publiquement par la suite peut également être considérée comme un facteur d'influence. Dès lors, chaque action pourrait être considérée comme étant réalisée sous influence. Il faudrait donc définir un indicateur de la force de cette influence en fonction des circonstances de l'espèce, afin de qualifier un niveau à partir duquel un individu agit librement, même en présence d'une contrainte minime.

96. Deuxièmement, si l'on cherche à obtenir une faculté d'autonomisation optimale, il est nécessaire de continuer l'analyse de sa structure en s'attachant à définir les conditions nécessaires à l'existence d'une volonté minimale, c'est-à-dire, pourvue des outils suffisants pour se construire. Par exemple, nous évoquions l'absence d'éducation sexuelle au point 63, qui pouvait restreindre la vie privée. C'est bien la volonté qui est atteinte, par le manque de connaissances suffisantes pour pouvoir développer une sexualité qui serait propre à l'individu en fonction de ses mœurs, et qui peut le rendre vulnérable sur le plan de sa santé. De la même manière, l'ignorance de l'existence d'une liberté individuelle prive la volonté de l'examen de son recours potentiel. Dans ce cas, n'existe-t-il pas, à l'instar du droit Allemand, une

extension du droit au respect de la vie privée vers un droit au développement personnel minimum ?

97. Nous pouvons mieux représenter cette problématique en prenant l'exemple d'une société où l'information et l'éducation serait totalement contrôlée. En réduisant les connaissances des individus, l'Etat serait capable, de manière imperceptible pour ces derniers, de contrôler les désirs d'une population. Dans ce cas-là, n'est-ce pas leur vie privée qui serait atteinte ? Sous une telle acception, le droit au respect de la vie privée implique une analyse à deux niveaux suivant l'approche phénoménologique de la formation de la volonté. Dans un premier temps, il faut que l'individu soit capable de désirer, et pour cela, il lui faut la connaissance. Dans un second temps, l'individu doit évaluer la possibilité de réaliser son désir dans son environnement. C'est, selon Aristote, le choix des moyens : « *Nous ne délibérons non pas sur les fins elles-mêmes, mais sur les moyens d'atteindre les fins. […]. Mais une fois qu'on a posé la fin, on examine comment et par quels moyens elle se réalisera ; et s'il apparaît qu'elle peut être produite par plusieurs moyens, on cherche lequel entraînera la réalisation la plus facile et la meilleur. […]. En effet, quand on délibère on semble procéder, dans la recherche et l'analyse dont nous venons de décrire la marche, comme dans la construction d'une figure […] et ce qui vient en dernier dans l'analyse est premier dans l'ordre de la génération. Si on se heurte à une impossibilité, on abandonne la recherche, par exemple, s'il nous faut de l'argent et qu'on ne puisse pas s'en procurer ; si au contraire une chose apparaît possible, on essaie d'agir* » [211]. Or à ce stade, il est possible de limiter cette recherche d'une manière indirecte en plaçant le sujet dans un état où celui-ci conclura faussement que l'action est difficile, voire impossible.

98. En prolongeant la recherche sur ces outils analytiques, le droit serait capable d'évaluer l'impact de n'importe quelle mesure sur le droit au respect de la vie privée, tel que nous l'avons défini. Pourtant, si nous pouvons faire le constat du respect de la volonté de l'individu, encore faut-il lui donner un périmètre d'exercice dont il pourra exclure les volontés extérieures.

211 Aristote, *Ethique à Nicomaque*, Vrin, 1 janvier 1994, p. 64.

Section 2

La protection du périmètre objectif de la vie privée

99. Si le droit au respect de la vie privée se définit comme une protection de l'autonomie décisionnelle, il faut aussi lui attribuer un périmètre dans lequel la volonté de l'individu prime sur celle de ses semblables. En cela, notre approche diffère du concept d'autodétermination mis en avant par une partie de la doctrine. Selon Yves Poullet et Antoinette Rouvroy, « *l'autodétermination individuelle présuppose que l'individu continue à disposer de sa liberté de décider d'agir ou de s'abstenir, et de la possibilité de suivre cette décision en pratique. Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée* »[212]. Appliquée au numérique, celle-ci devient une autodétermination informationnelle qui est « *le fait que le contrôle par un individu de l'information et des données produites à son propos est une condition, nécessaire mais, ajoutons, non suffisante, pour lui permettre de vivre une existence ne fut-ce que partiellement autodéterminée* » [213]. Pour Alexandre Flueckiger : « *retranscrit en vocabulaire plus moderne, le droit à l'autodétermination en matière de données personnelles doit être considéré comme un moyen de garantir le droit à la liberté individuelle et plus précisément à la protection de la sphère privée* » [214].

100. En suivant cette approche, la doctrine part du principe que le droit des données à caractère personnel est consubstantiel au droit à la vie privée, défini par la capacité

212 Poullet Yves, Rouvroy Antoinette, *Le Droit à l'Autodétermination Informationnelle et la valeur du développement personnel. Une Réévaluation de l'importance de la vie privée pour la démocratie*, Etat de Droit et virtualité, Ed. Karim Benyekhlef & Pierre Trudel, Montréal: thémis, 2009, p. 175.

213 Ibid, p. 171.

214 Flueckiger Alexandre, *L'Autodétermination en Matière de Données Personnelles : un Droit (plus si) Fondamental à l'Ere Digitale ou Nouveau Droit de Propriété ?*, Pratique juridique actuelle, 2013, vol. 22, p. 843.

d'autodétermination d'un individu. Dès lors, une personne doit nécessairement être en mesure de contrôler la captation d'informations qui est réalisée à son égard. Or cette pensée théorique fait face à une véritable limitation dans les faits. En liant l'autodétermination à la liberté d'agir dans un environnement donné, on élimine la distinction entre la formation d'une volonté et la possibilité de la suivre en pratique. En effet, une personne ne possède pas toujours la capacité juridique de contrôler une captation d'informations. Celle-ci peut être le résultat d'une législation contraignante, à l'instar du nouveau fichier des Titres Electroniques Sécurisés (TES) qui va regrouper l'ensemble des informations civiles des Français[215] et dont la possibilité de refuser cette nouvelle norme au niveau individuel est absente. Dans cette acception, la définition du droit au respect de la vie privée uniquement au regard de la capacité d'autodétermination génère une difficulté d'application par son approche individualiste.

101. De fait, si l'on définit la vie privée simplement au regard de la capacité d'autodétermination, il est évident que le citoyen n'en possède pas. Pour reprendre l'exemple du fichier TES, le citoyen ne dispose pas du choix de refuser la collecte ni l'agrégation des différents fichiers. En réalité, la capacité d'autodétermination informationnelle ne dépend plus de lui, mais de la société, ce qui est incompatible avec l'approche individualiste de la notion. Cela crée une difficulté structurelle dans l'appréciation d'une mesure attentatoire à la vie privée puisque par définition, toute mesure viendrait limiter la capacité d'autodétermination ainsi définie. Il est donc nécessaire d'introduire une certaine plasticité en rejetant l'approche individualiste pour se rapprocher d'une définition holistique intégrant la société.

102. Pour pallier cet écart structurel, entre l'approche individualiste de la notion de vie privée et l'approche sociétale, il faut nécessairement passer par une scission du concept. Ainsi, notre proposition de définir le droit au respect de la vie privée comme une protection de la faculté d'autonomisation à laquelle auquel on rattache un périmètre d'autonomie décisionnelle réunie ces deux acceptions. Appliquée au cas du fichier TES, on peut apprécier successivement l'impact de la création d'un tel fichier sur la capacité des individus à acquérir une autonomie décisionnelle, puis juger du périmètre décisionnel qu'offre la société à

215 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, texte n°18.

l'individu en l'espèce. La vie privée, selon cette définition gigogne, permet d'intégrer la volonté sociétale sans réduire celle de l'individu, à la différence du concept d'autodétermination informationnelle.

103. Si le premier élément de définition est à rattacher au droit fondamental, le second devient la modalité d'exercice de celui-ci dans une société donnée. De fait, si la capacité décisionnelle individuelle est nécessaire dans toute société, son expression est soumise à une limite acceptable, fixée collectivement. Selon la Cour de Cassation, « *l'exercice de cette liberté peut être soumis à certaines conditions, restrictions ou sanctions prévues par la loi qui constituent des mesures nécessaires dans une société démocratique, notamment pour la protection des droits d'autrui ; que tel est l'objet des dispositions du Code pénal […] relatives à l'atteinte à l'intimité de la vie privée* » [216]. Une telle prise en compte permet de donner une certaine plasticité à la notion de vie privée, pouvant s'adapter à chaque situation en fonction des mœurs, tout en gardant une définition unique préservant le droit fondamental. Elle comprend également l'idée qu'une réduction du périmètre accordé à l'expression d'une volonté puisse affecter la capacité d'une personne à désirer celle-ci. Tout dépend donc, du périmètre décisionnel que l'on offre réellement à l'individu. Le respect du droit à la vie privée va donc dépendre de l'équilibre entre ses deux aspects : autonomie décisionnelle et périmètre d'exercice de celle-ci.

104. Si la première partie cherchait à définir la notion de vie privée, il nous reste à analyser le périmètre décisionnel offert par le droit, donnant à la personne la capacité d'imposer sa volonté aux autres. On peut s'appuyer pour cela sur la définition d'intimité de la vie privée. En effet, il existe une difficulté inhérente à la notion de vie privée : sa définition matérielle. Dès lors, afin de faciliter l'application de la protection, le droit au respect de la vie privée a fait l'objet d'une objectivisation législative, doctrinale et jurisprudentielle à partir du concept d'intimité de la vie privée.

105. Par exemple, selon la Cour d'Appel de Paris statuant sur la divulgation d'informations relative à l'état de santé psychologique d'un candidat à une élection municipale, la « *vie privée s'entend de l'intimité de l'être humain en ses divers éléments afférents notamment à sa vie familiale, à sa vie sentimentale, à son image ou à son état de santé qui doivent être*

216 Cass. Crim, 20 octobre 1998, n°97-84621, Bull. Crim, 1998, n°264, p. 765.

respectés en ce qu'ils ont trait à l'aspect le plus secret de la personne »[217]. Cette position jurisprudentielle s'appuie sur l'article 226-1 du Code Pénal qui ne sanctionne pas directement les atteintes à la vie privée, mais les atteintes à l'intimité de la vie privée. Est puni « *d'un an d'emprisonnement et de 45 000 euro d'amende le fait, au moyen d'un procédé quelconque, volontairement, de porter atteinte à l'intimité de la vie privé* »[218].

106. Autant sur le plan législatif que jurisprudentiel, il s'agit là d'une distinction sémantique importante entre vie privée et intimité de la vie privée, puisque cette dernière ne représente pas la notion dans son ensemble. Pour François Cordier : « *Le délit d'atteinte à l'intimité de la vie privée ne recouvre qu'un champ beaucoup plus restreint et n'a pour objet que de sanctionner les intrusions frauduleuses dans la vie privée d'autrui* »[219]. Cela représente une volonté législative de réduire la portée du concept à une définition matériellement appréciable par les juges du fond. Selon Nathalie Cazé-Gaillarde : « *la référence légale à l'intimité de la vie privée s'explique par le souci de limiter la protection pénale à ce qui touche au plus intime de la vie privée. La garde des Sceaux avait ainsi affirmé que le projet de loi de 1970 tendait à fixer une limite au domaine de la vie privée, objet de protection légale, en précisant que seules les atteintes à l'intimité de la vie privé seraient sanctionnées sur la plan civil ou pénal* »[220]. On peut remarquer toutefois que cette distinction est absente de l'article 9 du Code Civil, qui consacre simplement la protection de la vie privée. Il existe une certaine confusion entre les notions qui entraine une difficulté à définir le fondement d'une action, civile ou pénale, selon l'atteinte constatée.

107. En liant le concept de vie privée au respect de la volonté d'un individu, autorisant ou non une intrusion, le concept d'intimité de la vie privée définit un périmètre décisionnel pour l'individu. Se cristallise une objectivisation du droit au respect de la vie privée sous deux acceptions : le périmètre décisionnel physique de la vie privée (1), puis le périmètre décisionnel informationnel accordé à l'individu (2).

217 CA. Paris, 5 décembre 1997, D. 1998, IR 32, Gaz. Pal. 1998.1, somm. 234.
218 Code Penal, Article 226-1.
219 Cordier François, *L'Atteinte à l'Intimité de la Vie Privée en Droit Pénal et les Médias*, Legicom, 4/1999, n°20, 1999, p. 85.
220 Cazé-Gaillarde Nathalie, *Vie Privée (Atteintes à la)*, Répertoire de droit pénal et de procédure pénale, Dalloz, Octobre 2014, point 20.

1 – La protection du périmètre décisionnel physique

108. On peut concevoir le concept d'intimité de la vie privée comme une définition physique de l'espace décisionnel d'une personne. À l'intérieur de ce périmètre, l'individu est en mesure de décider pour lui-même, quitte à exclure les volontés étrangères. Cela nécessite la réunion de deux critères : une reconnaissance de la libre disposition de cet espace et une protection contre les ingérences externes. Selon cette conception, seuls deux objets juridiques peuvent constituer un périmètre décisionnel physique relatif à la vie privée : le corps humain et le domicile.

a) Le corps humain

109. Le premier sanctuaire physique de cette intimité, en tant que périmètre décisionnel physique, est le corps humain. Selon l'article 16-3 du code civil, créé par la loi du 29 juillet 1994[221], puis modifié par la loi du 7 août 2004 sur la bioéthique[222] : « *Il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autru*i ». L'individu est maître de son propre corps. Par conséquent, « *le consentement de l'intéressé doit être recueilli préalablement, hors le cas ou son état rend nécessaire une intervention thérapeutique à laquelle il n'est pas à même de consentir* » [223]. Cela s'accompagne d'une protection plus large définie par l'article 16-1 du Code civil, tout d'abord avec une définition universelle de la portée de la notion, « *chacun a droit au respect de son corps* », puis avec l'établissement du principe d'indisposition du corps humain, «*le corps humain est inviolable* »[224].

110. La conjugaison de ces principes avec ceux de l'article 8 de la Convention Européenne des droits de l'homme[225] conduisent à une interprétation excessivement stricte de la capacité

221 Loi n°94-653 du 29 juillet 1994, *relative au corps humain*, JORF n°175 du 30 juillet 1994, p. 11056.
222 Loi n°2004-800 du 6 août 2004, *relative à la bioéthique*, JORF n°182 du 7 août 2004, p. 14040, texte n°1.
223 Code civil, article 16-3.
224 Code civil, article 16-1.
225 Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales telle qu'amendée par les Protocoles n°11 et n°14, Rome, 4 novembre 1950, article 8.

de disposer de son propre corps. Ainsi, dans son arrêt Aycaguer c. France[226], la CEDH a considéré que le refus de se soumettre à un prélèvement biologique destiné à l'enregistrement de son profil dans un fichier de Police était légitime si les conditions de conservation des informations, dudit fichier, n'était pas suffisantes pour garantir l'équilibre entre les intérêts publics et privés en jeu. En l'espèce: « *la Cour estime que le régime actuel de conservation des profils ADN dans le FNAEG, auquel le requérant s'est opposé en refusant le prélèvement, n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante à l'intéressé. Elle ne traduit donc pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Ces éléments suffisent à la Cour pour conclure que l'État défendeur a outrepassé sa marge d'appréciation en la matière. Dès lors, la condamnation pénale du requérant pour avoir refusé de se soumettre au prélèvement destiné à l'enregistrement de son profil dans le FNAEG s'analyse en une atteinte disproportionnée à son droit au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique* » [227].

111. Cela semble signifier que même si une mesure attentatoire à la vie privée prise par un Etat est légitime[228], dans le cas du corps humain, l'individu est capable de s'opposer à celle-ci si les conditions factuelles de conservation des informations n'offrent pas une protection suffisante. Par extension, on peut penser que l'individu est capable, au moins juridiquement, de s'opposer à toute intervention sur son corps si les conditions dans lesquelles cette action serait conduite lui semblent constituer une atteinte excessive et disproportionnée. Cela s'ajoute au fait que ce droit subjectif de la personnalité est un droit intransmissible, indisponible et imprescriptible.

112. De fait, le corps humain est intransmissible aux héritiers puisque selon l'article 3 de la loi du 15 novembre 1887 sur la liberté des funérailles, la volonté du défunt doit être respectée en ce qui concerne les conditions de ses funérailles[229]. Cela veut dire qu'un individu dispose de son corps jusque dans la mort, et que toute personne qui donnerait aux funérailles un caractère contraire aux dispositions prévues s'exposerait aux sanctions définies à l'article 433-21-1 du code pénal. Dans ce cadre, seul l'article 225-17 du code pénal autorise les héritiers à

226 CEDH, 22 juin 2017, *Aycaguer c. France*, n°8806/12.
227 Ibid.
228 Au regard des exigences posées par l'article 8 de la Convention Européenne des Droits de l'Homme.
229 Code civil, article 16-1.

agir en justice dans le cas d'une atteinte à l'intégrité du cadavre[230]. De plus, le corps humain est indisponible parce que, s'il est possible de monnayer l'utilisation indirecte de son corps par contrat comme dans le cas d'une autorisation de photographier, « *ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial* »[231]. Par conséquent : « *les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles* » [232]. De même « *aucune rémunération ne peut être allouée à celui qui se prête à une expérimentation sur sa personne, au prélèvement d'élément de son corps ou à la collecte de produits de celui-ci* » [233]. Enfin, il s'agit d'un droit imprescriptible conformément à l'article 16-1-1 du Code Civil qui énonce : « *le respect dû au corps humain ne cesse pas avec la mort* » [234]. En effet, à la suite de sa modification par la loi du 19 décembre 2008 relative à la législation funéraire[235] : « *les restes des personnes décédées, y compris les cendres de celles dont le corps a donné lieu à crémation, doivent être traités avec respect, dignité et décence* » [236].

113. Par extension, l'individu est libre d'utiliser son corps comme il le souhaite, notamment en ce qui concerne les relations sexuelles. La cour Européenne des droits de l'Homme a, dès 1981, considéré qu'une législation nationale condamnant les pratiques homosexuelles était contraire au droit au respect de la vie privée : « *par son maintien en vigueur, la législation attaquée représente une ingérence permanente dans l'exercice du droit du requérant au respect de sa vie privée (laquelle comprend sa vie sexuelle) au sens de l'article 8 par.1 (art.8.1)* »[237]. Or, la Cour va considérer cette ingérence comme non proportionnée au but cherché. Elle s'appuie pour cela sur l'impact de la décision sur la capacité de l'individu à décider pour lui-même. Ainsi, « *dans la situation personnelle de l'intéressé, elle se répercute de manière constante et directe, par sa seule existence, sur la vie privée de celui-ci : ou il la*

230 Article 225-17 du code pénal : « *toute atteinte à l'intégrité du cadavre, par quelque moyen que ce soit, est punie d'un an d'emprisonnement et de 15 000 euros d'amende. La violation ou la profanation, par quelque moyen que ce soit, de tombeaux, de sépultures, d'urnes cinéraires ou de monuments édifiés à la mémoire des morts est punie d'un an d'emprisonnement et de 15 000 euros d'amende. La peine est portée à deux ans d'emprisonnement et à 30 000 euros d'amende lorsque les infractions définies à l'alinéa précédent on été accompagnées d'atteinte à l'intégrité du cadavre* ».

231 Code civil, article 16-1, al. 3.

232 Code civil, article 16-5.

233 Code civil, article 16-6.

234 Code civil, article 16-1-1.

235 Loi n°2008-1350 du 19 décembre 2008, *relative à la législation funéraire*, JORF n°0296 du 20 décembre 2008, p. 19538, texte n°1.

236 Code civil, article 16-1-1.

237 CEDH, 22 octobre 1981, *Dudgeon c. Royaume Uni*, n°3198034/51.

respecte et s'abstient de se livrer –même en privé avec des hommes consentants – à des actes sexuels prohibés auxquels l'inclinent ses tendances homosexuelles, ou il en accomplit et s'expose à des poursuites pénales » [238]. Celle-ci confirmera sa jurisprudence dans plusieurs affaires[239], au point de créer un principe de non-discrimination à l'égard de l'orientation sexuelle[240].

114. Cette liberté de disposer de son corps s'entend comme une liberté quasiment absolue, allant jusqu'à la possibilité de considérer, dans le cas d'une personne en fin de vie souhaitant un suicide assisté pour éviter des souffrances futures, qu'il s'agit avant tout de respecter le principe « *de l'autonomie personnelle, au sens du droit d'opérer des choix concernant son propres corps* »[241]. En l'espèce, la Cour constate que « *la requérante est empêchée par la loi d'exercer son choix d'éviter ce qui, à ses yeux, constituera une fin de vie indigne et pénible. La Cour ne peut exclure que cela représente une atteinte au droit de l'intéressée au respect de sa vie privée, au sens de l'article 8 § 1 de la Convention* » [242]. Cette possibilité de disposer de son corps s'applique également dans le cas des relations sadomasochistes qui, librement consenties, ne peuvent être pénalement réprimées. Selon l'arrêt de la CEDH KA et AD c. Belgique : « *le droit d'entretenir des relations sexuelles découle du droit de disposer de son corps, partie intégrante de la notion d'autonomie personnelle. A cet égard,* « *la faculté pour chacun de mener sa vie comme il l'entend peut également inclure la possibilité de s'adonner à des activités perçues comme étant d'une nature physiquement ou moralement dommageables ou dangereuse pour sa personne. En d'autres termes, la notion d'autonomie personnelle peut s'entendre au sens du droit d'opérer des choix concernant son propre corps* » [243] » [244]. Seuls des motifs particulièrement graves justifieraient une intervention législative en la matière.

115. Ces ingérences sont tolérées par la Cour Européenne dans la mesure où celles-ci sont prévues par une loi, et qu'elles constituent dans une société démocratique des mesures nécessaires à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la

238 Ibid.
239 v. CEDH, 22 avril 1993, *Modinos c. Chypre*, n°7/1992/352/426 ; CEDH, 9 janvier 2003, *L et V c. Autriche*, n°39392/92.
240 CEDH, 21 décembre 1999, *Salgueiro da Silva Mouta c. Portugal*, n°33290/96, point 36.
241 CEDH, 29 juillet 2002, *Pretty c. Royaume Uni*, n° 2346/02
242 Ibid.
243 CEDH, 29 juillet 2002, *Pretty c. Royaume Uni*, n° 2346/02.
244 CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, n° 42758/98 et 45558/99.

défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui[245]. Les Etats membres ont sur ce point une marge d'appréciation : « *grâce à leurs contacts directs et constants avec les forces vives de leur pays, les autorités de l'Etat se trouvent en principe mieux placées que le juge international pour se prononcer sur le contenu précis de ces exigences comme sur la « nécessité » d'une « restriction » ou « sanction » destinée à y répondre* » [246]. Cependant, il existe une obligation positive de protéger les individus dans tous les aspects de leur vie privée, notamment en pénalisant les atteintes physiques et morales sur mineurs[247], ou en poursuivant « *de manière effective tout acte sexuel non consensuel, même si la victime n'a pas opposé de résistance physique* » [248].

116. Par conséquent, le corps humain représente le premier bastion d'une autonomie décisionnelle quasiment totale, dérivant du droit au respect de la vie privée. Dans ce contexte, une logique similaire s'applique au second espace physique décisionnel relatif à la vie privée, le domicile.

b) Le domicile

117. Selon le Conseil Constitutionnel, il existe un principe d'inviolabilité du domicile en vertu de l'article 66 de la Constitution[249], qui confie à l'autorité judiciaire la sauvegarde de la liberté individuelle sous tous ses aspects[250]. Toute intrusion à l'intérieur de celui-ci, ou maintien à l'aide de manœuvres, menaces, voies de fait ou contraintes, hors des cas où la loi le permet, est puni d'un an d'emprisonnement et de 15 000 euro d'amende selon l'article 226-4 du Code pénal récemment modifié par la loi du 24 juin 2015 tendant à préciser l'infraction de violation de domicile[251]. De même, en s'appuyant sur la dimension civiliste du droit au

245 Convention Européenne des Droits de l'Homme, telle qu'amendée par les Protocoles n°11 et14, complétée par le Protocole additionnel et les Protocoles n°4, 6, 7,12 et 13, article 8 al. 2.
246 CEDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, n°5493/72, para. 48.
247 CEDH, 2 décembre 2008, *KU c. Finlande*, n°2872/02.
248 CEDH, 4 décembre 2003, *M.C. c. Bulgarie*, n°39272/98.
249 Constitution du 4 octobre 1958, JORF du 5 octobre 1958, p9151.
250 Conseil Constitutionnel, Décision n° 83-164 DC du 29 décembre 1983, *Loi de finances pour 1984*, Rec. p. 67 - Journal officiel du 30 décembre 1983, p. 3871.
251 Article 226-4, Code pénal, tel que modifié par la loi n°2015-714 du 24 juin 2015 tendant à préciser l'infraction de violation de domicile, JORF n°0145 du 25 juin 2015 10410 texte n°1.

respect de la vie privée, la Cour de Cassation peut sanctionner toute intrusion dans le domicile sur le fondement de l'article 9 du Code Civil[252].

118. De jurisprudence constante, chaque intrusion à l'intérieur du domicile, en l'absence de l'accord de la personne, est considérée comme une ingérence dans l'exercice du droit au respect du domicile[253]. Cependant, il est possible d'atténuer ce principe à travers des dispositions législatives[254] selon la même logique utilisée par la Cour Européenne des Droits de l'Homme pour justifier une atteinte à l'intégrité corporelle. Celle-ci utilise le fondement de l'article 8 alinéas 2 de la Convention Européenne des Droits de l'Homme, relatif à la vie privée, pour analyser toute mesure restrictive portant sur le droit au respect du domicile[255]. La qualification de la licéité de l'atteinte se fait selon la même procédure : s'il existe une ingérence prévue par la loi poursuivant un but légitime, nécessaire dans une société démocratique, et si celle-ci est proportionnée. Le contrôle est étendu à la mise en œuvre de ces dispositions. Par conséquent: « *l'exercice des pouvoirs permettant de porter atteinte au domicile et à la vie privée doit demeurer confiné dans des limites raisonnables afin que soit réduit au minimum l'impact que de telles mesures peuvent avoir sur la sphère personnelle – y compris les aspects de sécurité et de bien-être – de l'individu telle que garantit l'article 8* » [256].

119. Il existe donc, concernant le corps humain, une protection juridique du respect de la volonté de la personne relative à son domicile. Le périmètre accordé à cette volonté concerne en premier lieu la désignation de celui-ci[257], même dans le cadre professionnel[258], et seules des limites d'usage liées à des circonstances particulières à certains milieux professionnels peuvent être tolérées[259]. Par conséquent, la qualification de domicile diffère de la domiciliation civiliste rattachée à un lieu d'habitation où la jouissance est réservée à un

252 Cass. Civ., 25 février 2004, n°02-18081, Bull. civ. 2004, III, n°41, p.729.
253 v. CEDH, 24 juillet 2008, *André et autres c. France*, n°18603/03.
254 Conseil Constitutionnel, Décision n°96-377 DC du 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 - Journal officiel du 23 juillet 1996, p. 11108.
255 Convention Européenne des Droits de l'Homme, telle qu'amendée par les Protocoles n°11 et14, complétée par le Protocole additionnel et les Protocoles n°4, 6, 7,12 et 13, article 8 al. 2.
256 CEDH, 18 juillet 2016, *Keegan c. Royaume Uni*, n°28867/03.
257 CEDH, 11 janvier 1991, *Buckley c. Royaume-Uni*, n°20348/92.
258 Cass. Com., 7 octobre 1997, n°95-30146, Bull. Com. IV, n°247, p. 215.
259 Notamment en ce qui concerne la réception au domicile d'un mineur par un encadrant scolaire, voir en ce sens : Cass. Soc., 13 janvier 2009, n°07-43282, Bull. Soc. 2009, V, n°3.

individu qui en possède le droit. Selon la Cour Européenne, la notion est indépendante des classifications en droit interne[260], et s'apparente aux lieux dans lesquels l'individu réside de manière habituelle[261], sans tenir compte de la licéité de cette occupation[262]. Il peut s'agir d'un véhicule[263] ou même d'un domicile commercial ou professionnel[264]. Enfin, ce respect de la volonté de la personne s'applique à la manière dont celui-ci souhaite utiliser son domicile[265], qu'il soit locataire[266] ou propriétaire[267]. Pour ce dernier, l'article 544 code civil va jusqu'à disposer que « *la propriété est un droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements* »[268].

120. Finalement, le domicile correspond, comme le corps humain, à un périmètre physique d'indépendance de la personne face à la société, à l'intérieur duquel il est capable d'exclure et d'imposer sa volonté. Relevant de la liberté individuelle, cet espace bénéficie d'un régime particulièrement protecteur de la vie privée en limitant strictement les atteintes et en punissant les intrusions. Ce régime repose principalement sur le respect de la volonté de la personne, en lui donnant une liberté presque absolue d'en jouir comme elle le souhaite. Cette latitude accordée au périmètre décisionnel physique de l'individu marque une véritable différence avec celle qu'on lui offre dans le cadre du périmètre décisionnel informationnel.

260 CEDH, 18 novembre 2014, *Prokopovich c. Russie*, n°58255/00.
261 Cass. Crim, 22 janvier 1997, n°95-81186, Bull. Crim, 1997, n°31 p.83.
262 Cass. Crim, 31 janvier 1914, S, 1916, 1, p. 59.
263 CEDH, 30 mai 1974, *X. c. Belgique*, n°5488-72.
264 CEDH, 21 janvier 2010, *Xavier Da Silveira c. France*, n°43757/05.
265 CEDH, 24 juillet 2003, *Karner c. Autriche*, n°40016/98.
266 Cass. Civ., 19 septembre 2012, n°10-12.024, AJDI 2012, p. 754.
267 CEDH, 13 juin 1979, *Marckx c. Belgique*, n°6833/74.
268 Article 544 du Code civil.

2 – La protection du périmètre décisionnel informationnel

121. Les citoyens bénéficient d'un pouvoir presque absolu de disposer de leur corps ou de leur domicile. Mais si la vie privée peut se concevoir comme un espace physique de protection, les informations que l'on peut extraire d'une personne et diffuser ensuite constituent un second moyen d'atteinte au droit au respect de la vie privée. Dès lors, il faut analyser de la même façon le périmètre décisionnel que le droit offre à l'individu pour définir la collecte et de la diffusion de ces informations.

122. Dans une approche objectiviste de la vie privée, si on laisse de côté la dimension physique de la vie privée que le droit réduit au corps humain et au domicile, la vie privée possède une seconde dimension exclusivement informationnelle. Celle-ci commence par la maîtrise des éléments formant l'identité d'une personne. Dans la décision du 25 mars 1992, la CEDH a eu à juger de la légitimité d'une demande de changement de nom pour une personne transsexuelle[269]. En l'espèce, celle-ci invoquait une atteinte à sa vie privée puisque « *les documents officiels se multiplient : extraits de naissance, cartes d'identité informatisées, passeport des Communautés européennes, etc. Partant, un transsexuel ne saurait franchir une frontière, subir un contrôle d'identité ou accomplir l'une des multiples démarches de la vie quotidienne qui impliquent une justification d'identité, sans révéler la discordance entre son sexe légal et son sexe apparent* » [270]. De même « *un transsexuel ne pourrait donc cacher sa situation à un employeur potentiel et à son personnel administratif, ni dans les multiples occasions de la vie quotidienne où l'on doit la réalité et le montant de son salaire. […]*[271]. *Des difficultés en résulteraient pour l'insertion sociale et professionnelle des transsexuels* ». Enfin : « *la requérante traverserait des épreuves quotidiennes dans sa vie économique en ce que ses factures et ses chèques indiqueraient son sexe d'origine en sus des noms et prénoms* »[272]. Considérant ces éléments, la Cour conclura que cette personne se trouve bien « *quotidiennement placée dans une situation globale incompatible avec le respect de sa vie privée* »[273], en fondant sa décision sur une infraction à l'article 8 de la Convention.

269 CEDH, 25 mars 1992, *Botella c. France*, n°57/1990/248/319.
270 Ibid, point 59.
271 Ibid.
272 Ibid.
273 Ibid.

123. La Cour Européenne ira plus loin, en reconnaissant dans sa décision du 11 juillet 2002 « *qu'il peut y avoir une atteinte grave à la vie privée lorsque le droit interne est incompatible avec un aspect important de l'identité personnelle* » [274]. Elle consacre une obligation positive des Etats membres à garantir la possibilité pour les transsexuels de faire changer leur état civil. Dès lors, même si un tel changement peut être limité aux cas où la modification chirurgicale a effectivement eu lieu[275], cela vient s'ajouter à la possibilité en droit Français de changer de prénom en faisant état d'un intérêt légitime[276].

124. Cette faculté décisionnelle s'applique à l'identité civile d'une personne, capable d'imposer un éventuel changement aux autorités étatiques, dans les conditions définies précédemment. Cependant, si nous avons observé la possibilité de changer cette identité, il faut également analyser les conditions dans lesquelles les informations de la personne peuvent être utilisées. Or, celles-ci dépassent le cadre exclusif de l'identité, pour s'attacher à tout type d'information sur la personne.

125. Dans ce cadre plus large, le droit accorde à la personne une faculté de contrôler les informations que l'on peut extraire de sa personne. Même dans un espace public, le domaine de la vie privée s'étend : « *les photographies de M. X et de Mme Y, prises au tournoi de tennis de Monte-Carlo, à l'insu des intéressés avec un cadrage les isolant du public environnant, ont été publiées et divulguées sans leur autorisation,[…]; que la vie sentimentale et affective comme les amours et l'état de grossesse, même apparent, de Mme Y, fussent-ils accompagnées de gestes visibles du public en des lieux particulièrement fréquentés par des personnes jouissant d'une notoriété momentanée, ou circonstancielle, qu'il appartient à chacun de gérer à sa guise et selon des conditions préalablement discutées avec tout support médiatique désireux de répondre à la curiosité réelle ou suscitée du public, constituaient une atteinte due au respect de sa vie privée* » [277].

126. Cela se rapproche d'un droit à la tranquillité selon Jean Carbonnier[278], qui s'étend à toute personne « *quels que soient son rang, sa naissance, sa fortune, ses fonctions présentes*

274 CEDH, gr. ch., 11 juillet 2002, *Christine Goodwin c. Royaume-Uni*, n°28957/95.
275 TGI. Paris, 30 novembre 1988.
276 Cass. Ass. Plén. 11 décembre 1992, n°91-11.900, Bull. civ. 1992 A.P. n°13 p. 27.
277 Cass. Civ. 2e, 10 mars 2004, n°01-15322, Bull. Civ. 2004, n°117, p. 97.
278 Carbonnier Jean, *Droit Civil*, vol. 1, PUF, 8 octobre 2004, p. 518.

ou à venir » [279]. De même : « *la circonstance que la personne visée exerce une activité d'homme public ne saurait autoriser une intrusion quelconque dans ce qui constitue la vie privée au respect de laquelle chacun se doit* » [280]. La seule exception pouvant venir réduire la portée de ce principe réside dans le droit à l'information, dont la Cour Européenne protège l'utilisation au nom de la liberté d'expression en tentant de trouver un point d'équilibre entre les deux notions: « *si la presse ne doit pas franchir certaines limites, concernant notamment la protection de la réputation et des droits d'autrui, il lui incombe néanmoins de communiquer, dans le respect de ses devoirs et de ses responsabilités, des informations et des idées sur toutes les questions d'intérêt général et de publier des photos. A cette fonction s'ajoute le droit, pour le public, d'en recevoir* » [281].

127. Selon l'arrêt Von Hannover c. Allemagne du 24 juin 2005, « *la Cour considère qu'il convient d'opérer une distinction fondamentale entre un reportage relatant des faits – même controversés – susceptibles de contribuer à un débat dans une société démocratique, se rapportant à des personnalités politiques, dans l'exercice de leurs fonctions officielles par exemple, et un reportage sur les détails de la vie privée d'une personne* » [282]. Ce faisant, « *la Cour considère que l'élément déterminant, lors de la mise en balance de la protection de la vie privée et de la liberté d'expression, doit résider dans la contribution que les photos et articles publiés apportent au débat d'intérêt général* » [283]. Mais la qualité de l'apport au débat d'intérêt général est difficile à évaluer pour chaque cas d'espèce, d'autant que cette approche ne prenait pas en compte la notoriété de la personne concernée ou le mode d'obtention des informations. Un référentiel plus précis fut donc développé dans l'arrêt Axel Springer Ag c. Allemagne du 7 février 2012, en établissant une liste de critères nécessaires à la mise en balance du droit à la liberté d'expression avec celui du respect de la vie privée : la contribution à un débat d'intérêt général, la notoriété de la personne visée et l'objet du reportage, le comportement antérieur de la personne concernée, le mode d'obtention des informations et leur véracité, le contenu, la forme et les répercussions de la publication, la gravité de la sanction imposée[284].

279 Cass. Civ. 1re, 23 octobre 1990, n°89-13.163, Bull. Civ. 1990, I, n°222, p. 158.
280 Cass. Civ. 1re, 13 avril 1988, n°86-15524, Bull. Civ. 1988, I, n°98, p. 67.
281 CEDH, 24 juin 2004, *Von Hannover c. Allemagne*, n°59320/00, considérant 42.
282 Ibid. Considérant 63.
283 Ibid, Considérant 64.
284 CEDH, gr. ch., 7 février 2012, *Axel Springer Ag c. Allemagne*, n°39954/08, considérant 89 et suivants.

128. Cet équilibre va dépendre grandement des conditions dans lesquelles les informations ont été recueillies, et surtout, si le périmètre décisionnel physique a été compromis. Dans le cadre de l'affaire Bettencourt par exemple, la Cour de cassation a considéré « *que la liberté de recevoir et communiquer des informations peut être soumise à des restrictions prévues par la loi et nécessaires, dans une société démocratique […] qu'il en va particulièrement ainsi du droit au respect de la vie privée […] lequel, en outre, étant sa protection au domicile de chacun ; qu'il s'ensuit que si, dans une telle société, et pour garantir cet objectif, la loi pénale prohibe et sanctionne le fait d'y porter volontairement atteinte, au moyen d'un procédé de captation, sans le consentement de leur auteur, de paroles prononcées à titre privée ou confidentiel, comme de les faire connaitre du public, le recours à ces derniers procédés constitue un trouble manifestement illicite, que ne sauraient justifier la liberté de la presse ou sa contribution alléguée à un débat d'intérêt général* » [285]. Il existe donc bien, même dans le cadre de la liberté d'expression, une limite physique applicable à la captation d'informations dans le domicile de la personne.

129. Au final, et à l'exception du cas particulier s'appliquant dans le cadre d'une collecte d'informations ayant eu lieu dans le domicile, tout citoyen dispose d'un périmètre décisionnel relatif aux informations issues de sa personne. Même si une partie de cette faculté est tempérée par l'exception journalistique, l'individu reste maître de la façon dont les tiers peuvent rapporter des informations qui lui sont liées. Mais aujourd'hui, une grande partie des informations échangées sont numériques. Pour comprendre toute l'extension de cette capacité décisionnelle, il faut donc analyser le droit applicable aux données à caractère personnel.

Conclusion

130. Si on considère le droit au respect de la vie privée comme une protection de la faculté d'autonomisation à laquelle on associe un périmètre décisionnel, le corps humain et le domicile en sont le sanctuaire physique. L'identité et les informations que l'on peut extraire de la personne en sont la dimension informationnelle, même si le périmètre décisionnel en l'espèce est fortement réduit.

285 Cass. Civ 1re, 15 janvier 2015, n°14-12200, non publié au bulletin.

131. Selon cette observation, le législateur aurait pu considérer que le droit au respect de la vie privée dans l'innovation technologique relevait d'une approche analytique similaire, en conférant aux supports informatiques un statut protégé équivalent au domicile, et une protection des données similaire à celle applicable à l'identité. Sur l'aspect physique par exemple, on peut citer le principe novateur utilisé par la Cour Constitutionnelle Allemande lorsqu'il s'agissait de qualifier la licéité des perquisitions informatiques[286]. Celle-ci a érigé un principe de garantie de la confidentialité et de l'intégrité des systèmes informatiques, en le rattachant au droit général de la personnalité. Selon l'analyse de Marcel Moritz : « *la Cour confère à ce principe une portée potentiellement très large en ne définissant pas la notion de système informatique. Il faut donc considérer que sont visés tous les systèmes traitant électroniquement des données. Sont par exemple concernés, outre les ordinateurs à proprement parler, les téléphones mobiles, comportant de multiples fonctions ou encore les agendas électroniques* »[287].

132. De plus, afin que la protection soit la plus efficace possible : *« il suffit que la perquisition soit susceptible de fournir un ensemble d'informations personnelles, sans que doive être rapportée la preuve que le système comportait effectivement de telles informations. En d'autres termes, le système est protégé par référence à ses capacités de stockage et de traitement, et non par rapport à son contenu réel* »[288]. Cependant, il semble que les législateurs Français et Européens aient décidé de réduire la portée de la protection de la vie privée dans l'innovation technologique en la faisant s'appliquer uniquement à sa partie informationnelle, à travers la notion de données à caractère personnel.

286 Bundesverfassungsgericht, 27 février 2008, aff. 1 BvR 370/07 et BVR 595/07.
287 Moritz Marcel, *Les Perquisitions en Ligne et la Surveillance d'Internet*, Revue Le Lamy Droit de l'Immatériel, n°41, 1er août 2008, pp. 52-62.
288 Ibid.

Chapitre 2

La protection offerte par le régime applicable aux données à caractère personnel

*

133. La France ne fut pas la première nation à légiférer sur le droit des données à caractère personnel. Avant elle, le Land de Hesse en Allemagne en 1970[289], la Suède en 1973[290] et les Etats Unis en janvier 1974[291] avaient déjà pris des dispositions en la matière. Pourtant, le Gouvernement Français avait, dès 1969, demandé au Conseil d'Etat d'analyser les atteintes éventuelles que l'informatique pouvait causer aux libertés individuelles[292]. Cela s'inscrivait dans un contexte plus large de prise en compte des nécessités de la protection de la vie privée par les législateurs, avec le vote sur la loi du 17 juillet 1970 qui inscrivit le principe du respect de la vie privée dans l'article 9 du code civil[293]. Cela n'empêcha pas la loi 24 juin 1970, prévoyant la création d'un fichier centralisé et automatisé des permis de conduire, de n'intégrer aucune mesure tendant à minimiser son impact au regard de la protection de la vie privée[294], et cela, alors même que la dangerosité d'un fichier centralisée était établie[295].

289 Datenschutz, Landesdatenschutezgesetz Vom 07/10/1970, Hessen.
290 DATALAG (Svensk Forfattningssamling [SFS] 1973 :289.
291 Privacy Act of 1974, 5, U.S.C.
292 Foyer Jean, *Rapport n°3125 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur le projet de loi n°2516 relatif à l'informatique et aux libertés par M. Foyer*, Assemblée Nationale, Annexe au procès-verbal de la séance du 4 octobre 1977, p. 12.
293 Loi °70-643 du 17 juillet 1970*, tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 19 juillet 1970 p. 6751.
294 Loi n°70-539 du 24 juin 1970, *sur la centralisation de la documentation relative à la circulation routière*, JORF du 25 juin 1970, p. 5963.
295 v. Foyer Jean, *Rapport n°3125 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur le projet de loi n°2516 relatif à l'informatique et aux libertés par M. Foyer*, Assemblée Nationale, Annexe au procès-verbal de la séance du 4 octobre 1977, p. 12.

134. Comme le souligne le rapport d'information sénatorial du député Jean Foyer de 1975 : « *l'étendue des services rendus par l'ordinateur à la cause du progrès scientifique et technique semblerait devoir susciter, de prime abord, un panégyrique sans réserve. […]. Il semble que la réalité soit plus nuancée et cette technique nous parait être, comme la langue d'Esope, la meilleure ou la pire des choses selon l'usage que l'on en fait* »[296]. Cette dichotomie entre bénéfices et risques fut particulièrement discutée à la suite de la publication d'un article du Monde en 1974 faisant état de la mise en place d'un système automatisé des fichiers administratifs et du répertoire des individus (SAFARI)[297]. Devant les critiques, le Gouvernement créa une commission chargée de proposer des mesures garantissant le développement de l'informatique dans le respect de la vie privée[298].

135. Ses conclusions seront en grande partie reprises par la loi du 6 janvier 1978[299], qui instaura en France le premier cadre législatif de protection de la vie privée dans la société de l'information. Celle-ci énonce dans son article premier: « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » [300]. Or, cette formulation laissait un doute quant à la nature du droit à la protection des données. En prenant appuis sur notre approche précédente, ce nouveau droit pouvait s'intégrer dans notre conception de la définition de vie privée à plusieurs niveaux. D'abord en tant qu'extension de la protection de la faculté d'autonomisation d'un individu, lui conférant un droit numérique à consulter des informations et à communiquer sans surveillance. En établissant, par exemple, un périmètre de protection autour de ses moyens de communication à l'instar du domicile. Puis en lui octroyant un périmètre décisionnel informationnel quant à l'utilisation de ses données.

296 Ibid, p. 6.
297 Boucher Philippe, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.
298 v. Chenot Bernard, Aydalot Maurice, Tricot Bernard et. al., *Rapport de la Commission de l'Informatique et des libertés*, Paris, 1975, 128 p.
299 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227.
300 Ibid, article 1.

136. Toutefois, le Conseil d'Etat[301], puis définitivement la loi sur la république numérique[302], rattachèrent le droit à la protection des données à caractère personnel à la notion d'autodétermination informationnelle. Ainsi, dans le nouvel article 1 de la loi informatique et libertés modifiée dispose : « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* »[303]. Ce faisant, le droit a opéré une translation conceptuelle imparfaite, en considérant que la matérialisation de la vie privée dans le numérique se réduisait à la capacité de décider du partage de ses informations. Par conséquent, avant même d'analyser le dispositif de protection des données à caractère personnel, on peut déplorer la réduction conceptuelle et juridique qui laisse de côté un pan important du concept de vie privée, notamment sur les aspects de développement personnel et d'impact psychosociologique.

137. Pour comprendre l'ampleur de ce phénomène, il convient de définir avec précision le régime applicable aux données à caractère personnel (Section 1), avant de démontrer la réduction conceptuelle du droit au respect de la vie privée dans l'innovation technologique (Section 2).

301 Conseil d'Etat, *Etude annuelle 2014, Le numérique et les droits fondamentaux*, Doc. Fr, 2014, coll. Les rapports du Conseil d'Etat, p. 264.

302 Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

303 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, modifiée par la Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

Section 1

Le régime applicable aux données à caractère personnel

138. Le régime protecteur de la vie privée dans le numérique s'applique aux *données à caractère personnel*. Selon l'article 2 de la loi informatique et libertés modifiée : « *constitue une données à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »[304]. Pour plus de précision, le règlement général sur la protection des données ajoute à cette liste : « *des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » [305].

139. Selon le Groupe de travail sur l'article 29 (G29), cette définition ne s'applique pas seulement aux informations objectives « *telles qu'une particularité sanguine de la personne concernée* »[306], mais aussi aux « *informations subjectives sous forme d'avis ou d'appréciations* » [307]. Le format importe peu : « *qu'elles soient alphabétiques, numériques, graphiques, photographiques ou acoustiques* » [308]. De même, *« pour être considérées comme des données à caractère personnel, il n'est pas nécessaire que ces informations soient vraies ou prouvées* »[309]. On peut donc considérer que tout type d'information numérique, quel que

304 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

305 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 4.

306 Groupe de Travail « Article 29 » *sur le concept de données à caractère personnel*, adopté le 20 juin 2007, 0148/07/FR, WP136, p. 7.

307 Ibid.

308 Ibid.

309 Ibid.

soit sa méthode de conservation, puisse être une donnée à caractère personnel. Dans ce cadre, c'est le lien de rattachement à la personne qui va être déterminant.

140. Il faut dans un premier temps savoir si le traitement « *concerne* » une personne. Pour cela, le G29 a développé, dans son avis du 20 juin 2007, une méthodologie reposant sur trois facteurs : le contenu, la finalité et le résultat[310]. Le traitement concerne la personne si les données *ont trait à la personne*, si celles-ci *sont utilisées pour produire une décision qui peut l'affecter*, ou si le résultat du traitement *peut l'impacter* d'une manière quelconque. Ces trois éléments entrainent l'application du régime, dès lors que l'un d'eux est caractérisé. À titre d'exemple, un système de localisation de véhicules de transport de personnes n'intègre pas nécessairement l'identité des chauffeurs, et ne produit pas de décision à leur encontre. Néanmoins, le résultat d'un tel traitement peut les affecter en dénonçant les excès de vitesse. Dans un pareil cas, le traitement concerne bien les chauffeurs, et justifie l'application potentielle du régime.

141. Car l'application du régime dépend ensuite d'un second élément : la faculté d'isoler une identité à partir des données. Pour reprendre notre exemple précédent, il s'agira de savoir si les chauffeurs peuvent être individuellement liés à un excès de vitesse particulier. Dans ce contexte, si la personne concernée est directement identifiée par son nom, la donnée est bien évidement identifiante. Mais la même solution s'applique dans le cadre d'un traitement qui identifierait indirectement les personnes concernées, en utilisant un numéro unique pour chaque personne, dont le lien indirect avec l'identité serait ensuite assuré par un second fichier. Cela s'applique, par exemple, aux fichiers de numéros de téléphones traités par les opérateurs téléphoniques, puisse ce que ceux-ci connaissent l'identité d'une personne ayant souscrit à un abonnement téléphonique.

142. Une difficulté peut survenir si l'identité n'est pas présente en tant que telle dans le traitement, que ce soit directement ou indirectement par interconnexion. Selon l'article 2 de la loi informatique et libertés modifiée : « *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou tout autre personne* »[311].

310 Ibid. p10.

311 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier

Dans ce cadre, ce n'est pas seulement les données dont dispose le responsable de traitement qui sont visées, mais bien l'ensemble des données que lui-même ou un tiers pourrait utiliser pour retrouver une identité à partir des données initiales. Ainsi, le considérant 26 du RGPD précise que « *pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci* »[312].

143. Cette méthodologie s'applique facilement lorsqu'il s'agit de faire un rapprochement entre plusieurs informations suffisamment précises, ou si l'information fragmentée est équivoque. À titre d'exemple, le G29 propose « *l'actuel premier ministre espagnol* »[313], ou des informations détaillées et catégorielles telles que « *la tranche d'âge, l'origine régionale etc.* » [314]. Par une approche au cas par cas, il faut donc déterminer s'il existe un moyen de corréler les informations de la base de données avec d'autres informations disponibles pour retrouver une identité, ainsi que le degré de techniques ou de connaissances que cela requiert. S'il s'avère qu'une telle corrélation est « *raisonnablement* » possible, l'identité est réputée identifiable indirectement. Toute la difficulté de la qualification tient donc dans la capacité des juges du fond à évaluer concrètement la faisabilité d'une telle opération.

144. Dans ce contexte, un niveau de complexité supplémentaire apparait dans l'évaluation des données techniques. Pour ce type d'informations, l'analyse des moyens « *susceptibles d'être raisonnablement mis en œuvre* » [315] pour retrouver l'identité de la personne est délicate. Pour le comprendre, on peut observer le point d'achoppement juridique qu'a constitué la qualification de l'adresse IP[316] comme données à caractère personnel. Si, dès les années 2000

1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

312 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, considérant 26.

313 Groupe de Travail « Article 29 » *sur le concept de données à caractère personnel*, adopté le 20 juin 2007, 0148/07/FR, WP136, p. 15.

314 Ibid.

315 Directive 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel n° L281 du 23 novembre 1995, p0031-0050, considérant 26.

316 Adresse Internet Protocol

le G29 avait qualifié, « *sans l'ombre d'un doute* »[317], les adresses IP dynamiques de données à caractère personnel, la justice Française a rejeté une telle approche à plusieurs reprises malgré les avis de la CNIL[318]. Ainsi même en 2015, la Cour d'Appel de Rennes rejetait la qualification au motif que l'adresse IP, composée d'une série de chiffres, se rapporte à un ordinateur et non à l'utilisateur. Selon son analyse, celle-ci ne permet pas de retrouver l'identité du propriétaire. Par conséquent, la personne concernée n'est pas identifiable au sens de la loi informatique et libertés car il n'existe pas de moyens de retrouver son identité[319].

145. Pour comprendre cette hésitation, il faut se reporter à la nature technique de l'adresse IP. En effet, celle-ci ne désigne pas une personne mais un numéro d'identification, provisoire ou pérenne, attribué à un dispositif de télécommunication numérique. L'attribution se fait selon un schéma technique contrôlé par l'ICANN[320], et chaque fournisseur d'accès transmet ce numéro d'identification à ses abonnés. Pour des raisons techniques, la désignation numérique de cette adresse comporte une partie variable, ainsi qu'une partie fixe désignant l'opérateur réseau et la zone géographique. Cette dernière peut être plus ou moins précise, selon la densité du maillage réseau. La corrélation entre l'identité du propriétaire et une adresse IP n'est connue, normalement[321], que par le fournisseur d'accès. Une analyse purement technique conclurait donc que cette donnée n'est pas une donnée identifiante en tant que telle. Toutefois, il faut intégrer dans ce schéma l'entière granularité des agents intervenant dans l'accès aux informations sur internet. Ainsi, un réseau social sur lequel les utilisateurs seraient identifiés dispose à la fois de l'identité de l'utilisateur enregistré et de l'adresse IP de l'ordinateur qu'il utilise pour se connecter.

146. Dès lors, on pourrait penser, à tort, que la qualification juridique d'une donnée technique telle que l'adresse IP dépend essentiellement des conditions matérielles du

317 Groupe de Travail « Article 29 » sur la protection des données, *Document de travail sur le respect de la vie privée sur internet, Une approche Européenne intégrée sur la protection des données en ligne*, adopté le 21 novembre 2000, 5063/00/FR/Final, WP37, p. 22.

318 La CNIL a rappelé dans sa communication du 2 août 2007 qu'une adresse IP était une donnée à caractère personnel, en réponse à la décision du 15 mai 2007 de la Cour d'Appel de Paris qui en donnait une interprétation différente. Pourtant, dans sa décision postérieure en date du 13 janvier 2009, la chambre criminelle de la Cour de Cassation refusait une nouvelle fois la qualification. v. Cass. Soc., 13 janvier 2009, n°07-43282, Bull. Soc. 2009, V, n°3.

319 CA Rennes, 28 avril 2015.

320 Internet Corporation for Assigned Names and Numbers

321 En l'absence de dispositif technique d'interception et d'intrusion dont la complexité technique relève de moyens étatiques ou privés extrêmement sophistiqués.

traitement et de la nature du responsable de traitement visé. Sous une telle perspective, la décision de la Cour d'Appel de Rennes parait justifiée. Cependant, on peut y opposer deux arguments. Tout d'abord, la décision ne tient pas compte de la diversité des moyens techniques permettant l'intrusion dans un système de traitement automatisé de données. Ensuite, il s'agit d'une interprétation erronée du champ applicable au critère de « *moyens à disposition* », dont la CNIL a manqué de rappeler l'importance dans ses précédentes décisions en la matière[322], et que la Cour de Justice a su expliquer dans sa décision du 19 octobre 2016 portant sur la licéité d'un traitement de données réalisé par un fournisseur de service à partir des données d'IP dynamique de ses usagers non enregistrés[323].

147. En l'espèce, la Cour entame son analyse en effectuant une distinction entre adresse IP statique, et adresse IP dynamique. Sur ce point, la Cour rappelle « *qu'il est constant qu'une adresse IP dynamique ne constitue pas une information se rapportant à une personne physique identifiée, dans la mesure où une telle adresse ne révèle pas directement l'identité de la personne physique propriétaire de l'ordinateur à partir duquel la consultation d'un site internet a lieu ni celle d'une autre personne qui pourrait utiliser cet ordinateur* » [324]. En vertu de l'approche au cas par cas engendrée par la formulation de la directive 95/46/CE[325] relative à l'applicabilité du régime aux données à caractère personnel, il convient donc dans un second temps « *de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* »[326].

148. Pour ce faire, la Cour rappelle « *qu'il n'est pas requis que toutes les informations permettant d'identifier la personne concernée doivent se trouver entre les mains d'une seule*

322 À titre d'exemple, on peut citer son appréciation dans l'affaire des panneaux publicitaires interprétant le comportement des passants, ou concernant l'affaire des Google Car et des captations d'adresses MAC et WI-FI v. respectivement, Commission Nationale de l'Informatique et des Libertés, *Avis du 19 avril 2010 sur la publicité comportementale* ; Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2011-035 du 17 mars 2011 *prononçant une sanction pécuniaire à l'encontre de la société X*, Publiée sur Légifrance le 13 décembre 2016.

323 CJUE, 19 octobre 2016, *Breyer c. Bundesrepublik Deutschland*, aff. C-582/14.

324 Ibid, point 38.

325 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, considérant 26.

326 Ibid, point 42.

personne »[327]. Or, elle constate « *qu'en vertu d'une disposition législative, le fournisseur de service de média est autorisé, en cas d'attaque informatique, à obtenir auprès du fournisseur d'accès l'identité de la personne titulaire de l'abonnement utilisé par l'adresse IP relevée* » [328]. Par conséquent : « *une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet rend accessible au public constitue, à l'égard dudit fournisseur, une données à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet de cette personne* » [329].

149. En suivant cette analyse, la qualification d'une donnée en donnée à caractère personnel dépend de la possibilité, juridique ou technique, d'obtenir l'identité d'une personne dont un responsable de traitement détient une donnée non nominative, par corrélation d'informations disponibles chez lui ou chez des tiers. Le seul fait que cette possibilité existe sur le plan juridique la rend identifiante, et l'analyse de la complexité des moyens à mettre en œuvre ne concerne que l'acquisition technique. À la lumière de cette conclusion, la dernière décision de la Cour de Cassation en date du 3 novembre 2016 reconnaissant la qualifie de données personnelle l'adresse IP parait moins nuancée : « *les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personne* » [330]. S'agit-il désormais d'une affirmation indépendante du contexte, ou d'une interprétation réduite de la méthodologie de la qualification des données à caractère personnel ? La seule certitude réside dans sa clarté à l'heure de définir les conditions relatives aux modalités du traitement (1) et les droits conférés à la personne concernée (2) à l'aube de l'application prochaine du RGDP.

327 Ibid, point 43.
328 Ibid, point 47.
329 Ibid, point 47.
330 Cass. Civ., 3 novembre 2016, n°1184, ECLI:FR:CCASS:2016:C101184.

1 – Les conditions relatives aux modalités du traitement

150. Le périmètre de la protection du droit au respect de la vie privée concernant les données à caractère personnel s'applique aux traitements de données. Selon l'article 2 de la loi informatique et libertés modifiée : « *constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* »[331]. Cette liste est étendue par le règlement Européen qui y ajoute dans son article 4 : « *la structuration [et] la limitation* » [332].

151. À partir d'une telle acception, on peut considérer que c'est d'avantage la présence de données à caractère personnel que les conditions factuelles des opérations informatiques qui qualifie le traitement. À titre d'exemples, la jurisprudence a considéré qu'un dispositif d'écoute téléphonique peut être qualifié de traitement[333], de même que des vidéos de personnes physique[334], un service de renseignement téléphonique[335] ou la simple mention d'informations personnelles relative aux membres d'une association sur un site internet[336]. Cette qualification s'applique également si les données à caractère personnel subissent, de manière indifférenciée, les mêmes opérations que d'autres types de données[337]. La seule exception à cette applicabilité réside dans l'exception d'utilisation exclusivement personnelle, présente à l'article 2 de la loi du 6 janvier 1978, comme dans le cas de la conservation d'email

331 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

332 Règlement 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, 4 mai 2016, Journal officiel de l'Union Européenne, L 119/1, article 4.

333 TGI. Paris, 1ere ch., 4 avril 2006.

334 CJUE, 11 décembre 2011, *Frantisek Rynes c. Urad pro ochranu osobnich udaju*, aff. C-212/13.

335 CJUE gr. ch., 5 mai 2011, *Deutsche Telekom AG c/ Bundesrepublik Deutschland*, aff. C-543/09.

336 CJCE, 6 novembre 2003, *Bodil Lindqvist,* aff. C-101/01.

337 CJUE, gr. ch., 13 mai 2014, *Google Span SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12.

personnels[338]. En résumé, le régime de protection est applicable dès lors qu'une seule identité se trouve concernée[339] et qu'il s'agit bien d'un fichier, au sens de l'article 4 du RGDP, qui le définit comme : « *tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » [340].

152. Si l'applicabilité du régime est avérée, en fonction de la qualification de la présence de données à caractère personnel et d'un traitement de celle-ci non exclusivement personnel, les mesures de protections relatives aux modalités du traitement deviennent applicables en vertu de l'article 6 de la loi informatique et libertés[341]. Celles-ci sont cumulatives[342] et concernent respectivement : la loyauté et la licéité de la collecte (a), la finalité déterminée, explicite et légitime (b), la proportionnalité de la mise en œuvre du traitement (c), le caractère exact et complet des données traitées (d) et la durée de conservation données (e). De plus, il nous faut rappeler que la modification récente de la loi de 1978 par la loi sur la République numérique a introduit une obligation de sécurisation des données. Faisant état d'éléments techniques, cette disposition est étudiée en dehors de cette section, dans la partie I, titre II, chapitre I, section II. De même, le consentement est étudié dans la partie II.

a) La loyauté et la licéité de la collecte

153. Les obligations de loyauté et de licéité de la collecte peuvent s'apparenter à un principe de transparence, que le nouveau règlement général juxtapose à l'obligation de loyauté et de licéité[343]. Selon celui-ci : « *le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a*

338 Cass. Crim., 30 novembre 2011, n°10-81749, Bull. Crim. 2011, n°243.

339 Cass. Crim., 8 septembre 2015, n°15-85587, Bull. Crim. 2015, n°191.

340 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 4.

341 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 6.

342 CJCE, 20 mai 2003, *Österreichischer Rundfunk et a., aff. jtes*. C-465/00, C-138/01 et C-139/01, point 65.

343 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 5.

lieu, illustrée à l'aide d'éléments visuels » [344]. Ces principes s'apparentent à l'obligation d'information à destination des personnes concernées, notamment en ce qui concerne la finalité de la collecte. Ainsi, a été jugé contraire à ce principe, une collecte réalisée par le biais d'un sondage politique pour recueillir les emails des personnes susceptibles d'être de la même sensibilité politique que le sondeur[345]. De même, a été réputée déloyale une collecte indirecte réalisée par la gendarmerie nationale[346], ou un recueil d'information par le biais d'un automate sans consentement initial[347].

154. Ce principe de recueil licite, loyal et transparent des données à caractère personnel sert de support aux droits accordés à la personne concernée, dont le responsable de traitement doit assurer l'existence. Selon la CNIL : *« revêt toujours un caractère déloyal et illicite […] l'information postérieure à la communication de leurs données à caractère personnel, rendant de ce fait impossible l'opposition aux annonceurs au traitement de leurs données* » [348]. Cela s'étend également aux responsables de traitement sous-traitant, comme par exemple dans le cadre d'une collecte de données à partir de service tiers. Ainsi, dans sa décision du 12 mars 2014, le Conseil d'Etat a jugé qu'un traitement effectué par un annuaire en ligne dont les données étaient collectées à partir de services tiers était illicite au regard du manque d'information des personnes concernées, et cela malgré « *la circonstance que, dans le cadre de leur politique de confidentialité, certains de ces réseaux sociaux avaient averti leurs membres de la possible indexation de ces données par des moteurs de recherche ne saurait faire regarder ceux-là comme déjà informés* » [349]. Dès lors, les données « *n'ont pas été collectées de manière loyale et licite, faute de consentement explicite et éclairé des intéressés* ».

344 Ibid, considérant 58.

345 T. Corr. Nanterre, 4 juin 2004.

346 Commission Nationale de l'Informatique et des Libertés, Délibération n°81-120 du 15 décembre 1981 *portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile*, JORF du 15 décembre 1981, n°34, p. 1210.

347 Commission Nationale de l'Informatique et des Libertés, Délibération n°85-73 du 9 juin 1981 *portant modification de la délibération n°81-77 du 9 juin 1981 concernant une recommandation relative à la collecte et au traitement d'informations nominatives relatives à des opinions politiques, philosophiques ou religieuse ou faisant apparaitre les origines raciales ou les appartenances syndicales par les entreprises privées de sondage*, JORF du 28 janvier 1986, p. 1543.

348 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2011-193 du 28 juin 2011 *prononçant une sanction pécuniaire de 10 000€ à l'encontre de la société X*, Publiée sur Légifrance le 13 décembre 2016.

349 CE, 12 mars 2014, *Pages Jaunes Groupe*, n°353193, Mentionné dans les tables du Recueil Lebon, ECLI:FR:CESSR:2014:353193.20140312.

155. Concrètement, cette obligation impose au responsable de traitement de veiller aux conditions de recueil des données à caractère personnel, et particulièrement aux exigences relatives à la licéité du consentement préalable qui intègrent l'obligation d'information. Par exemple, selon l'arrêt du 30 décembre 2009 du Conseil d'Etat, n'est pas licite un traitement n'ayant pas réuni les conditions d'un consentement libre et éclairé dans le cadre d'une demande de prêt dans laquelle « *le client est invité à donner son accord au transfert d'information le concernant, […], avant qu'il lui soit répondu à sa demande de prêt ou de crédit ; que, d'autre part, la notice d'information qui lui est remise ne précise ni les données exactes qui seront transmises à la « centrale de crédit », ni les utilisation de ces données par les établissements qui en seront destinataires, ni le délai de conservation de ces données dans la « centrale de crédit ; qu'ainsi la Commission nationale de l'informatique et des libertés, en estimant que les conditions […] pour que le consentement de l'emprunteur soit libre et éclairé n'étaient pas réunies et, qu'en conséquence, les information sur la situation financière de ce dernier n'étaient pas recueillies de manière illicite, n'a pas fait une inexacte application des dispositions de la loi du 6 janvier 1978* » [350].

156. En cas de non-respect, le responsable de traitement encourt les sanctions administratives que la CNIL peut prononcer en vertu de l'article 45 de la loi informatique et libertés[351], qui vont de l'interruption de la mise en œuvre du traitement à la sanction financière. Celles-ci sont cumulables avec les dispositions pénales des articles 226-16 et suivants.

b) Finalité déterminée, explicite et légitime du traitement

157. Selon l'avis du G29, la finalité doit être claire et spécifique pour que les personnes concernées puissent prévoir avec suffisamment de fiabilité l'utilisation future de leurs données[352]. Ce principe relationnel entre la finalité déclarée du traitement et l'utilisation

350 CE, 30 décembre 2009, *Association SOS Racisme, GISTI et autres*, n° 312051, Rec. p. 538.

351 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 45.

352 « *If purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable. This brings legal certainty to the data subjects, and also to those processing personal data on behalf of the controller* ». Groupe de Travail « Article 29 » *opinion 03/2013 on purpose limitation*, adopted on 2 April 2013, 00569/13/EN, WP 203, p. 13.

effective des données fait d'ailleurs l'objet d'une attention particulière puisque le Conseil Constitutionnel l'examine au regard du principe constitutionnel de l'article 2 de la déclaration des droits de l'homme et du citoyen de 1789[353], et que le Conseil d'Etat peut apprécier cette cohérence[354].

158. La finalité doit être exprimée avec suffisamment de précision pour que les personnes concernées puissent « *comprendre la finalité réelle de la collecte de leurs données* » [355]. En cas de manquement : « *le caractère particulièrement vague de l'information conduit ainsi les personnes à délivrer un nombre important d'informations les concernant, en conséquence de quoi la formation restreinte considère que la collecte des données à caractère personnel auprès des personnes appelées est déloyale* » [356]. Dans ce contexte, une information générale sur le devenir des données ne saurait suffire. Ainsi, lors de l'examen de la fusion des règles de confidentialité des services de Google, la CNIL a considéré qu'en se bornant à définir la finalité comme une mesure permettant d'assurer « *le bon fonctionnement des services. L'information ainsi délivrée, par sa généralité, ne peut en tant que tel satisfaire à l'objectif d'information claire et complète des utilisateurs fixé par la loi* » [357]. Celle-ci a par ailleurs relevé « *qu'en application de la méthode d'information dite multi-strate retenue par la société, les utilisateurs peuvent prendre connaissance d'informations complémentaires en cliquant sur le lien correspondant à la rubrique En savoir plus, dans laquelle plusieurs finalités et diverses informations complémentaires sont mentionnées. Pour autant, l'information ainsi fournie à l'utilisateur, tout aussi générale, ne permet pas à celui-ci d'associer un type de cookie et une finalité au service qu'il utilise. Dès lors, cette information n'est pas suffisamment circonstanciée quant aux cookies liés au service que l'utilisateur va utiliser* » [358].

353 Conseil Constitutionnel, Décision n° 2008-562 DC du 21 février 2008, *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*, Rec. p. 89 – Journal officiel du 26 février 2008, p. 3272, texte n°2.

354 CE, 13 décembre 1999, *Caisse de crédit mutuel de Bain-Tresboeuf*, n° 197060, Rec. p. 397.

355 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2015-454 du 21 décembre 2015 *prononçant un avertissement public à l'encontre de la société Profils Seniors*, Publiée sur Légifrance le 15 janvier 2016.

356 Ibid.

357 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

358 Ibid.

159. De manière concrète, cette obligation se traduit par la nécessité pour le responsable de traitement d'établir, en amont de la collecte, une procédure d'information à destination des personnes concernées. Celle-ci va ensuite le lier dans l'utilisation ultérieure qu'il pourra faire des données. En cas de manquement, les sanctions administratives de la CNIL sont les mêmes qu'en cas de manquement à l'obligation de loyauté et de licéité de la collecte, et les sanctions pénales de l'article 226-21 du Code Pénal s'appliquent pour détournement de la finalité.

c) Proportionnalité de la mise en œuvre

160. Selon l'article 6 de la loi du 6 janvier 1978, les données collectées doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » [359]. Pour attester de cette qualité, le conseil d'Etat considère que les données, « *pour être regardées comme pertinentes au sens de l'article 6 de la loi du 6 janvier 1978, sont en adéquation avec la finalité du traitement et proportionnées à cette finalité* » [360]. Il faut que les données recueillies correspondent exactement aux objectifs du traitement, en conformité avec le principe de minimisation des données issue de la Privacy By Design-(PbD).

161. Cette minimisation implique une réduction du périmètre de captation des données proportionnée aux finalités du traitement, mais également un examen de la pertinence globale du système. Ainsi, un système biométrique ayant pour finalité l'accès à la cantine par les élèves peut paraitre proportionné, à première vue, étant donné qu'il est nécessaire d'identifier les élèves. Cependant, le recours à cette mesure est disproportionné puisqu'une méthode moins intrusive est possible[361]. De même, si une collecte de données personnelles concernant les fait contraires aux règles de l'entreprise correspond à la finalité d'informer la maison mère sur les agissements des collaborateurs : « *La Commission estime que le dispositif présenté est disproportionné au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une « alerte éthique ». Elle relève à*

359Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 6.

360 CE, 16 avril 2010, *Association Inter-LGBT*, n°320196, Rec. p. 146.

361 v. Commission Nationale de l'Informatique et des Libertés, Délibération n°00-015 du 21 mars 2000 *portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales*, Publiée sur Légifrance le 14 octobre 2015.

cet égard que d'autres moyens prévus par la loi existent d'ores et déjà afin de garantir le respect des dispositions légales et des règles fixées par l'entreprise (actions de sensibilisation par l'information et la formation des personnels, rôle d'audit et d'alerte des commissaires aux comptes en matière financière et comptable, saisine de l'inspection du travail ou des juridictions compétentes) »[362].

162. Cette analyse de la proportionnalité de la mesure comporte donc une part d'appréciation circonstancielle porteuse d'insécurité juridique. À titre d'exemple, on peut mentionner la différence d'approche retenue lors de l'examen de la licéité de la mise en œuvre d'un traitement de donné ayant pour finalité la constatation de délits de contrefaçon d'œuvres musicales sur les réseaux peer to peer impliquant une surveillance étendue du réseau. Selon la CNIL, ces traitements « *ne sont pas proportionnés à la finalité poursuivie dans la mesure où ils n'ont pas pour objet de permettre la réalisation d'actions ponctuelles strictement limitées aux besoins de la lutte contre la contrefaçon mais peuvent aboutir au contraire à une collecte massive de données à caractère personnel sur internet et à une surveillance exhaustive et continue des réseaux d'échanges de fichiers dénommées « peer to peer »* »[363].

163. Cependant, le Conseil d'Etat eu une analyse différente lorsque l'affaire fut portée devant sa juridiction : « *Considérant qu'il ressort toutefois des pièces du dossier que les traitements envisagés par les sociétés requérantes ne portaient simultanément que sur quelques-uns des protocoles « peer to peer » permettant l'échange des fichiers musicaux sur internet ; que si les sociétés requérantes s'étaient engagées à constituer une base commune de contrôle portant simultanément sur 10 000 titres musicaux, faisant l'objet d'une actualisation hebdomadaire à hauteur de 10 % des titres composant la base, il convient ; pour apprécier l'ampleur et la pertinence de ce dispositif de traitement, de le rapprocher, d'une part, du nombre de titres musicaux dont les sociétés requérantes ont pour mission d'assurer la protection et, d'autre part, de l'importance de la pratique des échanges de fichiers musicaux*

362 Commission Nationale de l'Informatique et des Libertés, Délibération n°2005-110 du 26 mai *2005 relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle*, Publiée sur Légifrance le 14 octobre 2014.

363 Commission Nationale de l'Informatique et des Libertés, Délibération n°2005-237 du 18 octobre 2005 *portant refus d'autorisation de la mise en œuvre par la Société civile des Producteurs de Phonogrammes en France (PPF) d'un traitement de données à caractère personnel, ayant pour finalités, d'une part, la constatation des délits de contrefaçons commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçons*, Publiée sur Légifrance le 14 octobre 2014.

sur « internet » ; que les sociétés d'auteurs, compositeurs requérantes ont chacune la charge de la protection des droits de plusieurs millions de titres musicaux ; que les sociétés requérantes évaluent en France, annuellement, sans être contredites sur ce point, à plusieurs centaines de millions de fichiers les échanges illégaux de titres musicaux dans le cadre de ces réseaux ; que par suite, en estimant que les traitements envisagés conduisaient à une surveillance exhaustive et continue des fichiers des réseaux d'échanges et ne pouvaient par conséquent être regardés comme proportionnés à la finalité poursuivie, la CNIL a entaché sa décision d'une erreur d'appréciation » [364]. En conséquence, la CNIL revint sur sa décision et autorisât les traitements dans ses délibérations datées du 8 et du 22 novembre 2007[365].

164. Ce pouvoir d'appréciation s'exerce au-delà des législations Françaises. En vertu de l'article 6 de la directive 95/46/CE[366], dont le nouveau règlement Européen a réduit la portée en exonérant les traitements effectués par les autorités publiques dans l'exécution de leurs missions[367], la Cour Européenne des Droits de l'Homme peut juger de la proportionnalité d'une collecte au regard de ce qui est acceptable dans une société démocratique. Par exemple, celle-ci a jugé que « *le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées […] ne traduit par un juste équilibre entre les intérêt publics et privés concurrents en jeu, et que l'Etat défenseur a outrepassé tout marge d'appréciation en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique* » [368].

364 CE, 23 mai 2007, *SACEM*, n°288149, Inédit au Rec.

365 v. Commission Nationale de l'Informatique et des Libertés*, Peer-to-Peer : la CNIL se tourne vers l'avenir*, 17 décembre 2007.

366 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, article 6.

367Règlement (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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 6.

368 CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, point 125.

165. Par conséquent, l'exigence de proportionnalité s'analyse comme un principe de minimisation de l'impact du traitement sur la vie privée des personnes concernées, de par ses données et son spectre, dont l'examen de sa pertinence fait partie intégrante.

d) Caractère exact et complet des données

166. Selon le considérant 39 du nouveau règlement Européen : « *il y a lieu de prendre toutes les mesures raisonnables afin de garantir que les données à caractère personnel qui sont inexactes sont rectifiées ou supprimées* » [369]. C'est ce que son article 5 nomme « *le principe d'exactitude* » [370]. Selon la CNIL, « *il consiste sans ambiguïté en une obligation de résultat en ce qu'il impose de garantir au responsable de traitement l'exactitude des données à caractère personnel qu'il traite en prenant toutes les mesures utiles afin de rectifier ou d'effacer les données inexactes* » [371]. Cependant aussi bien la Cour de cassation que la formulation du règlement laisse supposer qu'il s'agit d'avantage d'une obligation de moyen que de résultat[372]. Dès lors, selon Romain Perray : *« l'obligation d'exactitude et de mise à jour des données doit s'interpréter comme une obligation certes de moyens, mais une obligation renforcée* » [373].

167. Cette obligation s'apparente au droit de la personne concernée à accéder aux données et de faire rectifier ou effacer toute information que ne serait pas exacte. Présent dans l'article 15 du règlement général sur la protection des données, le droit d'accès de la personne concernée permet, entre autre, « *de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel* » [374]. En cas de manquement, les sanctions administratives et pénales sont similaires à celles imposées en cas de manquement à l'une des obligations relatives aux modalités du traitement.

369 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, Considérant 39.

370 Ibid. Article 5.

371 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2016-053 du 1 mars 2016 *prononçant un avertissement à l'encontre de la société NC Numéricâble*, Publiée sur Légifrance le 9 mars 2016.

372 Cass. Civ., 4 mai 2012, n°10-27208, Gaz. Pal. 17 mai 2012, n°138, p. 13.

373 Perray Romain, *Jurisclasseur Administratif*, Fasc. 274-20, 18 mai 2016, point 39.

374Règlement (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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 6.

e) La durée de conservation

168. Selon l'article 5 du règlement général sur la protection des données, les données à caractère personnel doivent être : « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » [375], reprenant ainsi la formulation de l'article 6 de la loi informatique et libertés modifiée[376]. Seules certaines exceptions à ce principe existent, telles que la conservation à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique, statistiques, historiques, dans la mesure où ces traitements respectent les garanties de l'article 89 du règlement général relatives à la pseudonimisation des données.

169. Si l'on peut penser, à première vue, que cette obligation constitue une protection efficace de la vie privée, la référence à la finalité du traitement comme seul moyen de détermination de la durée de conservation des données entraine l'effet inverse. De fait, il faut distinguer la période d'utilisation effective des données par les personnes concernées, par exemple à travers l'utilisation d'un service, et la durée de conservation postérieure à celle-ci, qu'effectuerait le service à des fins de valorisation. Selon la CNIL : « *la fixation de durées de conservation définies ne saurait avoir pour effet de supprimer des données des utilisateurs alors qu'eux-mêmes en auraient encore l'usage. […] Le point de départ d'une durée de conservation n'est pas fonction de la date de la collecte, mais bien de la suppression du compte utilisateur* » [377]. Seule la finalité du traitement définit la durée de conservation des informations. On peut donc penser qu'en théorie, une finalité de valorisation éternelle des données nécessite une conservation éternelle des données.

170. Pour pallier ce risque au regard de la vie privée, la CNIL a mis en place un critère d'appréciation de la proportionnalité de la durée de la conservation en rapport avec les finalités déclarées[378]. En vertu du principe de transparence, celle-ci devra être indiquée

375 Ibid., article 5.

376 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 6.

377 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

378 Pour des exemples d'utilisation du principe par la CNIL, v. Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction*

préalablement aux personnes concernées, et correspondre à une durée proportionnelle à la finalité et limitée dans le temps. Sa définition exacte va dépendre du secteur d'activité du responsable de traitement, en fonction de dispositions spécifiques, ou bien des délibérations de la CNIL en matière d'autorisation unique. A titre d'exemple, l'article R.10-13 du Code des Postes et des communications électroniques fixe à un an la conservation des données pour les opérateurs de télécommunication électroniques et l'article R.1221-26 du Code du travail fixe à cinq ans la conservation des mentions portées sur le registre unique du personnel. De même, dans le cadre de la prospection, la Commission fixe une durée de trois ans à compter de leur collecte ou du dernier contact pour conserver les données d'un non client[379]. Si cette durée de conservation n'est pas définie, une analyse de la proportionnalité devra être réalisée par le responsable de traitement. Dans ce cadre, il faudra se référer aux analyses des précédentes jurisprudences de la CNIL en la matière. Enfin, il est à noter qu'en cas d'obligations entre commerçants, la Cour de Cassation a considéré que la durée de conservation pouvait être réduite conventionnellement[380].

171. En cas de défaut de proportionnalité, le responsable du traitement risque de se voir appliquer les sanctions administratives et pénales définies précédemment pour défaut de respect des conditions de licéité du traitement. Cependant, le caractère particulier du critère de proportionnalité dans la conservation des données entraine bien souvent une analyse a posteriori du traitement. Dans ce cadre, en plus des sanctions habituelles, apparait un risque d'annulation rétroactif pour les traitements administratifs. Ainsi, le Conseil d'Etat a décidé d'annuler partiellement un décret de mise en œuvre d'un traitement de données relatif aux titres de séjour[381]. De même, la haute juridiction administrative a prononcé l'annulation pure et simple de l'acte de modification d'un traitement de données pour absence d'une durée de conservation[382]. Enfin, on peut rappeler que cette obligation est particulièrement importante au regard du droit à l'oubli, faisant partie des droits conférés à la personne concernée.

---

pécuniaire à l'encontre de la société Google Inc., Publiée sur Légifrance le 10 janvier 2016 ; Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-007 du 26 janvier 2016 *mettant en demeure les sociétés Fracebooks Inc. et Facebook Ireland*, Publiée sur Légifrance le 10 février 2016.

379 Commission Nationale de l'Informatique et des Libertés, Délibération n°2012-209 du 21 juin 2012 *portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (norme simplifiées n°48),* JORF du 13 juillet 2012, texte n°72.

380 Cass. Com., 21 mars 1995, n°93-12.383, Bull. Com. 1995, IV, n°92, p. 82.

381 CE, 30 décembre 2009, *Association SOS Racisme, GISTI et autres*, n° 312051, Rec. p. 538.

382 CE, 18 mars 2005, *Syndicat national de défense de l'exercice libéral de la médecine à l'hôpital*, n°238206, Rec. p. 49.

2 – Les droits conférés à la personne concernée

172. Le règlement général sur la protection des données introduit de nouvelles dispositions relatives aux droits des personnes concernées. Ceux-ci sont complémentaires avec les conditions relatives aux modalités du traitement, avec lesquelles elles forment le principal pilier du droit au respect de la vie privée dans la société de l'information. Ces droits sont respectivement le droit d'information et d'accès (a), le droit d'opposition, de rectification et d'effacement (b), le droit à la portabilité des données (c), étant toutefois limités selon certaines modalités (d).

a) Droit d'information et d'accès

173. Le droit à l'information, que l'on peut assimiler à l'exigence de transparence de la part du responsable de traitement à l'égard des personnes concernées inscrite dans le règlement général, trouve son origine dans l'article 32 de la loi informatique et libertés. Selon celui-ci : « *La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant : 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ; 2° De la finalité poursuivie par le traitement auquel les données sont destinées ; 3° Du caractère obligatoire ou facultatif des réponses ; 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ; 5° Des destinataires ou catégories de destinataires des données ; 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°* » [383]. L'obligation d'information s'applique de la même manière dans le cas où les données n'ont pas été recueillies directement auprès de la personne concernées, mais elle peut être circonstanciée en fonction du terminal utilisé. Ainsi : « *tout*

383 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 32.

abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : - de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; - des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle »[384]. Cependant, cette dernière disposition n'est pas applicable si la finalité du traitement est de faciliter la communication ou si celui-ci est strictement nécessaire à la fourniture d'un service demandé expressément par l'utilisateur.

174. Inversement, si le droit d'information intervient au moment de la procédure de recueil de consentement initial, le droit d'accès s'applique pendant toute la durée du traitement. Ce faisant, la personne concernée peut consulter l'ensemble des données qui sont à la disposition du responsable de traitement. Selon l'article 39 de la loi informatique et libertés : « *toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ; 2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; 3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ; 4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au*

384 Ibid.

sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle » [385].

175. Enfin, *« Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction* » [386]. Cela permet à la personne concernée d'effectuer elle-même un contrôle du traitement, en vérifiant que les données en possession du responsable de traitement aient bien été collectées de manière licite, avec son accord.

b) Droit de rectification, d'opposition, et d'effacement

176. En vertu de l'article 40 de la loi informatique et libertés : « *toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent* » [387]. Ce droit s'accompagne d'un droit d'opposition, pour des motifs légitimes, à ce que des données concernant la personne soient traitées. Selon l'article 38, celui-ci s'exerce sans frais, notamment lorsqu'il s'agit d'un traitement dont les finalités sont assimilables à de la prospection commerciale.

177. La combinaison de ce droit d'opposition et de rectification donne à la personne concernée un contrôle sur les données traitées par le responsable du traitement. Or, celui-ci a fait l'objet d'une extension progressive à partir de la décision de la Cour de Justice dans son arrêt du 13 mai 2014 contre Google Spain[388]. En l'espèce, un justiciable Espagnol demandait la suppression de certains résultats de Google Search qui, à partir de son nom, renvoyaient vers des articles faisant état de son lien avec une vente aux enchères immobilière, elle-même

385 Ibid. article 39.
386 Ibid. article 39.
387 Ibid. article 40.
388 CJUE, gr. ch., 13 mai 2014, *Google Span SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12.

liée à une saisie en recouvrement. La question qui se posait à la Cour était celle de savoir si le droit d'opposition, présent dans les articles 12 et 14 de la directive 95/46/CE était de nature à procurer à la personne concernée le droit de demander au moteur de recherche de supprimer les données le concernant menant à ces pages tierces. Or, selon son analyse : « *les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite* ».

178. La Cour de Justice consacre, par cette décision, l'exercice d'un « *droit à l'oubli* », permettant aux citoyens Européens de demander la suppression de certaines données par les moteurs de recherche. Cela se traduira par une modification de l'article 40 de la loi informatique et libertés par la loi sur la République numérique. Dorénavant : « *sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci* » [389]. Or, si cette modification ne concerne que les mineurs, le règlement général sur la protection des données étant cette faculté. Selon l'article 17 : « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique: a) les données*

389 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 40.

à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement; c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2; d) les données à caractère personnel ont fait l'objet d'un traitement illicite; e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis; f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 »[390]. Concrètement en 2018, la personne concernée sera en mesure de révoquer son consentement au traitement des données, selon des modalités qui s'apprécieront de manière circonstancielle, notamment au regard du droit à la liberté d'expression et d'information, du respect d'une obligation légale, ou pour des motifs d'intérêt public dans le domaine de la santé publique.

179. Cependant, la portée de ce droit reste, pour l'instant, circonscrite à l'espace Européen. Malgré la décision de la Cour Européenne à son encontre[391] ainsi que la sanction de la CNIL[392], Google a décidé de porter l'affaire devant le Conseil d'Etat, considérant que l'applicabilité du droit à l'oubli était territorialisée et n'avait pas vocation à engendrer une suppression des résultats sur l'ensemble de son service mondialisé. Le même débat agite les juridictions étrangères. En effet, la Cour suprême du Canada a récemment penché en faveur d'une application mondiale du droit à l'oubli concernant ses ressortissants dans sa décision en date du 28 juin 2017[393]. Dans ce contexte, l'analyse du Conseil d'Etat relative à la contestation de la décision de la CNIL par Google est particulièrement attendue.

390 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 17.

391 CJUE, gr. ch., 13 mai 2014, *Google Span SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12.

392 Commission Nationale de l'Informatique et des Liberté, Délibération n°2016-054 du 10 mars 2016 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc.,* Publiée sur Légifrance le 26 mars 2016.

393 Supreme court of Canada, 28 juin 2017, Google Inc v. Equuustek Solution Inc, 2017 SCC 34.

c) Droit à la portabilité des données

180. Le droit à la portabilité des données représente la faculté, pour la personne concernée, d'exporter ses données d'un service vers un autre. Selon l'avis du G29 : « *le nouveau droit à la portabilité des données vise à redonner le pouvoir aux personnes concernées en facilitant leur capacité à copier ou à transférer leurs données personnelles aisément vers d'autres services informatiques* »[394]. Absent de la directive 95/46/CE et de la loi informatique et libertés, ce nouveau droit s'appliquera dès 2018, en vertu de l'article 20 du RGPD. Selon celui-ci : *« les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque: a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b); et b) le traitement est effectué à l'aide de procédés automatisés* » [395]. De plus : « *lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible. L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers* » [396].

181. S'il est évident que cette initiative du législateur Européen facilite l'utilisation des outils numériques pour les utilisateurs, ce nouveau type d'interaction avec le responsable de

394 Traduction de l'auteur de : « *the new right to data portability aims at empowering data subjects regarding their own personal data as it facilitates their ability to move, copy, or transmit personal data easily from one IT environment to another* ». Groupe de Travail « Article 29 » sur la protection des données, *Guidelines on the right to data portability*, adopted on 13 December 2016, 16/EN, WP 242, p. 4.

395Règlement (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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 20.

396 Ibid.

traitement soulève de nombreuses problématiques. D'une part, comme l'admet le G29 dans son avis du 13 décembre 2016[397], cette faculté d'extraction des données comporte une part de risques en cas d'usurpation d'identité. Pour pallier cela, des informations supplémentaires peuvent être demandées afin de s'assurer de l'authenticité de la requête. D'autre part, la mise en œuvre d'une telle procédure nécessite des moyens techniques importants, d'abord dans la mise en œuvre d'une extraction de données, puis dans l'interconnexion avec un service tiers. Dans ce cadre, l'adoption de standards techniques, à travers l'adoption de la Privacy By Design (PbD), sera nécessaire[398].

d) Limitations

182. Il existe un certain nombre de limites à ces droits. La première étant l'applicabilité du régime de protection des données à caractère personnel, rejetée « *si les données à caractère personnel recueillies sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la CNIL* » [399]. De même, ces droits ne peuvent pas être invoqués s'il s'agit de « *données recueillies dans les conditions prévues […] et utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sureté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sureté, dans la mesure ou une telle limitation est nécessaire au respect des fins poursuivies par le traitement* » [400]. Cette exception existe également pour les traitements ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales.

183. Toutefois, le législateur a ménagé un droit d'accès indirect à ces informations. Ainsi, les articles 41 et 42 de la loi informatique et libertés autorisent, pour ces types de traitements, la personne concernée à faire une demande auprès de la Commission pour que celle-ci mène *« les investigations utiles et [pour] faire procéder aux modifications nécessaires* » [401]. De plus, « *lorsque la commission constate, en accord avec le responsable du traitement, que la*

397 Groupe de Travail « Article 29 » sur la protection des données, *Guidelines on the right to data portability*, adopted on 13 December 2016, 16/EN, WP 242, p. 11.
398 v. point 293 de cet ouvrage.
399 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 32.
400 Ibid.
401 Ibid. article 41.

communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant »[402].

184. Le RGPD intègre la même exception dans son article 23, ainsi que des nouvelles catégories de traitements, tels que les « *objectifs importants d'intérêt public général de l'Union ou d'un Etat membre, notamment un intérêt économique ou financier important de l'Union ou d'un Etat membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale* »[403]. Sont également ajoutés les traitements relatifs à la protection de l'indépendance de la justice et des procédure judiciaires, à la prévention et la détection des manquement à la déontologie des professions réglementées ainsi que les requêtes et les poursuites en la matière, les missions de contrôle d'inspection ou de règlement liée à l'exercice de l'autorité publique.

Conclusion

185. Le régime applicable aux données à caractère personnel définit un double périmètre de protection. Tout d'abord, il encadre strictement la façon dont un responsable de traitement peut acquérir et utiliser des données. Puis, il confère aux personnes concernées un certain nombre de droits tendant à leur garantir un contrôle optimal sur leurs données. Afin de s'assurer du respect de celui-ci, le législateur a placé au centre de ce nouvel écosystème juridique la Commission Nationale de l'Informatique et des libertés, autorité administrative indépendante dont les missions sont définies à l'article 11 de la loi informatique et libertés[404].

186. L'organisme est chargé d'informer l'ensemble des personnes concernées ainsi que les responsables de traitement de leurs droits et obligations, et veille à ce que les traitements mis en œuvre soient conformes au régime de protection. Dans ce but, la loi impose une procédure de déclaration systématique des différents traitements auprès de la Commission, qui sera en

402 Ibid. article 41.

403 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 23.

404 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 11.

mesure de vérifier l'adéquation entre les déclarations effectuées et la réalité des traitements dans la pratique. Cette procédure s'impose à l'ensemble des traitements de données à caractère personnel, hormis « *les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical : pour les seules données mentionnées [...] correspondant à l'objet de ladite association ou dudit organisme ; sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ; et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément* »[405]. À cette compétence, s'ajoute également un pouvoir d'autorisation préalable pour certains types de traitements[406].

187. La conjonction de ces deux éléments, régime protecteur et contrôle par une autorité dédiée, semble apporter à la personne concernée une protection suffisante dans le domaine numérique. Pourtant, la définition même du régime des données à caractère personnel relève d'un paradigme différent de celui du droit au respect de la vie privée, au risque de diminuer celle-ci dans la société de l'information.

405 Ibid, article 8.

406 Ibid, article 25 : « *Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 : Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ; Les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ; Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ; Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ; Les traitements automatisés ayant pour objet :l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ; l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ; Les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes ; Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ; 8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ; Par dérogation au 1° du I et aux 1° et 2° du II de l'article 27, les traitements qui portent sur des données à caractère personnel parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou qui requièrent une consultation de ce répertoire, lorsque ces traitements ont exclusivement des finalités de recherche scientifique ou historique, à la condition que le numéro d'inscription à ce répertoire ait préalablement fait l'objet d'une opération cryptographique lui substituant un code spécifique non signifiant, propre à chaque projet de recherche, ainsi que les traitements ayant comme finalité exclusive de réaliser cette opération cryptographique* ».

Section 2

La réduction conceptuelle du droit au respect de la vie privée dans l'innovation technologique

188. En définissant, puis en s'appuyant sur la notion centrale de données à caractère personnel, le régime a su matérialiser une part de ce que peut représenter la vie privée dans l'ère numérique. Ce faisant, le législateur a amputé une grande partie du concept de vie privée en réduisant considérablement son périmètre initial. Les aspects sociaux sont réduits à l'aune de l'individualisation de la notion, qui s'appuie principalement sur le consentement de la personne concernée dans le cadre de traitements privés, ou par sa volonté exprimée indirectement par ses représentants lors de la mise en œuvre des traitements administratifs ou régaliens. Concrètement, cela revient à limiter le droit au respect de la vie privée dans le numérique à un simple périmètre décisionnel informationnel.

189. Au centre de ce paradigme, on trouve l'idée que la transformation numérique est inéluctable, et que l'utilisation des données à caractère personnel est, par conséquent, nécessaire. Selon le considérant 6 du règlement général sur la protection des données : « *l'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités* » [407]. Cette observation amène donc le considérant suivant à juger que : « *ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à*

407 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, considérant 6.

l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques »[408].

190. Ce faisant, le législateur a manqué d'intégrer au régime applicable aux données à caractère personnel la question de l'autonomie décisionnelle de l'individu (1), au risque de basculer vers une forme de patrimonialisation des données à caractère personnel (2).

1 – L'absence de protection de la faculté d'autonomisation

191. Nous avons défini la vie privée comme une protection de la faculté d'autonomisation de l'individu associée à un périmètre décisionnel physique et informationnel, avant de constater que cette définition n'avait pas été transposée en totalité dans le régime protection des données à caractère personnel. Devenue une représentation matérielle du périmètre décisionnel informationnel de l'individu dans la société de l'information, la protection se trouve amputée de la majeure partie de ses attributs. Cela conduit le droit à ne protéger que partiellement l'individu, notamment au regard de la faculté d'autonomisation.

192. Selon la Cour Européenne des droits de l'Homme dans sa décision du 24 février 1998 : « *la sphère de la vie privée, […] couvre l'intégrité physique et morale d'une personne* »[409]. Par conséquent : « *la garantie offerte par l'article 8 de la Convention est principalement destinée à assurer le développement, sans ingérences extérieures, de la personnalité de chaque individu dans les relations avec ses semblables* »[410]. Tout comme dans l'affaire Niemietz, la Cour a considéré qu'il existe « *un droit pour l'individu de nouer et développer des relations avec ses semblables* ». Ainsi, « *le droit au respect de la vie privée assure à l'individu un domaine dans lequel il peut poursuivre librement le développement et l'accomplissement de sa personnalité* »[411].

408 Ibid, considérant 7.
409 CEDH, 24 février 1998, *Botta c/Italie*, n°21439/93.
410 Ibid.
411 CEDH, 12 juillet 1977, *Brüggeman et Scheuten c. RFA*, n° 6959/75.

193. En réduisant le concept de vie privée à sa dimension informationnelle, le régime applicable aux données à caractère personnel ne permet pas de qualifier l'impact d'un traitement de données sur la capacité de développement personnel. Celui-ci devient même un obstacle à cette analyse, en substituant l'étude de l'influence d'un traitement sur la capacité de développement d'un individu aux critères de validité du consentement donné ou au regard de la proportionnalité de celui-ci avec sa finalité. Que l'on considère le consentement ou la proportionnalité comme des critères de licéité suffisants ou non[412], ils sont inadaptés dans ce contexte. Pour illustrer cette problématique, on peut citer l'exemple classique et largement présent dans la littérature juridique et sociale, de l'impact potentiel d'une surveillance étatique (développé dans la partie I, titre II, chapitre I, section I). Cependant, l'étude des algorithmes de Facebook chargés de la présentation des informations sur sa plateforme présente un intérêt supérieur.

194. En l'espèce, le réseau social Facebook construit un profil à partir des données partagées ou extraites de l'internaute lors de sa navigation. Á partir de celles-ci, « *nous sommes en mesure de vous proposer nos services, de personnaliser nos contenus et de vous faire des suggestions en nous fondant sur les informations obtenues* »[413]. Cela conduit naturellement le site internet à afficher différentes informations en fonction de la sensibilité politique de l'utilisateur, comme le dévoile le projet Blue Feed Red Feed du Wall Street Journal, montrant la différence des contenus affichés entre un utilisateur libéral et un utilisateur conservateur Américain[414]. L'individu est alors enfermé dans ce qu'Eli Pariser décrit comme une bulle filtrante[415], dont l'influence peut aller jusqu'à s'interroger sur la capacité des algorithmes à décider du sort de l'élection du président de la première puissance mondiale[416].

412 v. Partie II

413 Facebook, Politique d'utilisation des données, disponible sur https://fr-fr.facebook.com/about/privacy (consulté le 01/07/17).

414 Keegan Jon, *Blue Feed, Red Feed*, Wall Street Journal, 18 May 2016, disponible sur http://graphics.wsj.com/blue-feed-red-feed/#/health-care (consulté le 01/09/17).

415 v. Pariser Eli, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 1 mars 2012, 304 p.

416 Szadkowski Michel, Leloup Damien, *Facebook, faiseur de rois de l'élection Américaine ?,* Le Monde, 14 novembre 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/11/14/facebook-faiseur-de-rois-de-l-election-americaine_5030959_4408996.html (consulté le 01/09/17).

195. Abreuvé d'informations similaires, celui-ci navigue dans un espace informationnel uniforme, dont l'influence est certaine. Ainsi, selon David Forest « *Les prix « dynamiques » fixés en fonction des informations recueillies sur la navigation d'une personne sont un exemple topique. Ce modèle prédictif réduit toujours davantage l'incertitude des comportements en les structurant par des recommandations, c'est le cas sur le site Amazon par exemple, et non par la contrainte visible. […]. En cela, l'algorithme est doté d'une « force normative », non pas juridique mais comprise comme un gouvernement des conduites ou, pour reprendre un concept des relations internationales, une manière de soft power* »[417].

196. Victime de la bulle informationnelle générée par les algorithmes de traitement de données à caractère personnel, l'utilisateur de la technologie voit, au moins partiellement, sa capacité de développement personnel réduite. Mais le régime ne peut dans sa forme actuelle attester de celle-ci si la licéité du consentement, dans les conditions définies, est retenue. Par conséquent, en réduisant le droit au respect de la vie privée à la portion congrue dans l'innovation numérique, le législateur génère un risque non négligeable d'influence massive sur les citoyens Européens à travers l'utilisation des technologies. Mais plus encore, si cette influence peut s'exercer sur les citoyens, elle peut aussi s'exercer sur les personnes chargées de l'autorité étatique.

197. En 2015, la Police Nationale s'est dotée d'un logiciel de prédiction du comportement délinquant. Selon Patrick Perrot, chef de la division analyse et investigation criminelle au service central du renseignement criminel : « *nous construisons un modèle basé sur les infractions entre 2008 et 2013. S'il est validé et se vérifie sur les faits de 2014, nous le projetons sur l'année 2015* »[418]. À partir de ces données, une prédiction de la date et du lieu de la prochaine infraction est définie, permettant aux forces de l'ordre de se rendre sur place avant sa réalisation potentielle. Cependant, ce type de traitement n'exploite pas dans son intégralité le potentiel du big data avec la numérisation croissante de nos outils de déplacements et de communications. Une course s'est alors engagée pour construire le premier logiciel holistique d'analyse du comportement délinquant. Dans ce contexte, la France cherche à se doter de logiciels plus puissants en agrégeant des sources plus diverses[419]

417 Forest David, *La Régulation des Algorithmes, entre Ethique et Droit*, Lamy Droit de l'Immatériel, 2014.

418 Perrot Patrick, déclaration recueillie par Molinié William, *Viols, agressions, cambriolages : le nouvel algorithme des gendarmes pour prédire le crime*, 20 minutes, 21 mai 2015.

419 Hourdeaux Jérome, *Gendarmes et Industriels Imaginent un Nouveau Logiciel pour Prédire le Crime*,

et Israël a déjà franchi le pas en 2016 en traitant des données en provenance du big data, tels que les réseaux sociaux et les différents services applicatifs, pour être en mesure de créer une alerte instantanée lorsqu'un comportement indique un passage à l'acte imminent en matière de terrorisme[420].

198. Ce basculement algorithmique dans la prédiction des infractions comporte un risque de catégorisation des citoyens par les forces de l'ordre. À partir d'une étude de terrain réalisée en partenariat avec le département de police de Boston, Jessica Saunders, Priscilla Hunt et John Hollywood sont parvenus à démontrer que le taux d'implication des personnes identifiées par le logiciel comme susceptibles d'être en lien avec des affaires de violences avec armes n'était pas supérieur à celui d'un groupe témoin. Cependant, ceux-ci étaient nettement plus ciblés par les forces de l'ordre[421]. De fait, ces algorithmes statistiques conduisent à une définition sociale des criminels, information qui conduit ensuite les activités policières à se focaliser d'avantage sur des profils particuliers. Selon une autre étude réalisée à Boston: *« l'effet de la schématisation raciale suggère une disparité dans le traitement des activités des forces de l'ordre basée sur la composition raciale des quartiers »*[422]. En engageant d'avantage d'actions sur une population particulière, le nombre d'activités illicites découvertes augmente. Ce phénomène entraine une accélération auto-générée du biais statistique, puisque l'engagement policier est alloué en fonction de celui-ci et qu'il en devient le principal moteur. Cela peut même aller jusqu'à générer de nouvelles infractions, en suscitant une hostilité de la population à l'égard des forces de police[423].

199. Sur le plan du régime des données à caractère personnel, aucune protection n'existe face à ce type de menace pour le citoyen. Bien sûr, l'application conjointe des dispositions des articles 8 et 10 de la loi informatique et libertés, restringents respectivement l'usage des

---

Médiapart, 25 mai 2015, disponible sur https://www.mediapart.fr/journal/france/250515/gendarmes-et-industriels-imaginent-un-nouveau-logiciel-pour-predire-le-crime?onglet=full (consulté le 01/09/17).

420 20 Minutes avec AFP, *Menace terroriste : Israël affirme avoir créé une technique pour identifier les « loups solitaires »*, 20 Minutes, 28 juillet 2016, disponible sur http://www.20minutes.fr/societe/1901367-20160728-menace-terroriste-israel-affirme-avoir-cree-technique-identifier-loups-solitaires (consulté le 01/09/17).

421 Saunders, J., Hunt, P. & Hollywood, J.S. J Exp Criminol (2016) 12: 347. doi:10.1007/s11292-016-9272-0

422 Traduction de l'auteur de : *« the pattern of race effects suggests evidence of disparate treatment in FIO activity based on neighborhood racial composition* ». Fagan Jeffrey, Braga Anthony et.al., *Final Report: An analysis of Race and Ethnicity Patterns in Boston Police Department Field Interrogation, Observation, Frisk, and/or Search Reports*, June 2015, p. 8.

423 v. U.S. Department of Justice, Civil Rights Division, *Investigation of the Baltimore city police department*, August 10 2016.

données sensibles et notamment raciales, ainsi que l'usage qui peut être fait d'un traitement automatisé produisant des effets juridique à l'égard d'une personne relativement à certains aspects de la personnalité. Mais les dispositions des articles 9, 25 et 26 de cette même loi autorisent, sous condition, ce type de traitement pour les besoins des forces régaliennes. De plus, la mise en œuvre de ces dispositifs ne nécessite qu'une procédure d'avis auprès de la CNIL, et d'une dose de proportionnalité entre les données collectées et les buts définis. Dans le contexte sécuritaire qui est le nôtre, les conditions d'une action socialisée des forces de l'ordre sont réunies.

200. Dans cet environnement juridique et social, seul un régime protecteur des données personnel intégrant l'impact sur l'autonomie décisionnelle est efficace. À défaut, un glissement algorithmique impactant les capacités décisionnelles des individus ne relève plus seulement de la science-fiction[424].

2 – Le risque de patrimonialisation du régime protecteur des données à caractère personnel

201. La transposition imparfaite de la protection du droit au respect de la vie privée dans le domaine numérique par le régime applicable aux données à caractère personnel entraine un risque d'objectivisation de la vie privée numérique. Ainsi, lorsque la Cour de Cassation déclare nulle une cessation de fichier de clientèle pour absence de déclaration du fichier auprès de la CNIL, elle reconnait implicitement la faculté de vendre un tel fichier si cette condition est respectée[425]. Par conséquent, la donnée acquise licitement entre dans le patrimoine du responsable de traitement, et devient même la principale source de valeur pour les industries numériques.

202. Pour comprendre le glissement de paradigme que peut représenter cette exploitation, on peut prendre en exemple la décision de la Cour de Cassation en date du 11 décembre 2008. En l'espèce, un mannequin avait signé un contrat relatif à l'exploitation de son image «*sous*

424 v. Orwell George, *1984*, Gallimard, 16 décembre 1972, 438 p. ; Dick Philip K., *Minority Report*, Folio, 4 juin 2009, 272 p.
425 Cass. Com., 25 mars 2013, n°12-17037.

toute ses formes, sauf contexte pornographiques, et par tous procédés techniques, aux fins d'illustration, de décoration, promotion, publicité, de toute association, société, produit ou service, par télévision, satellite, vidéocassettes, internet, multimédia, CD Rom, presse, sur tous supports, pour le monde entier et une durée de quinze ans, renouvelable par tacite reconduction » [426]. Celle-ci, considérant a posteriori le contrat abusif, assigna la société en nullité de la convention et paiement de dommage et intérêt. Cependant, selon l'analyse de la Cour, « *les dispositions de l'article 9 du Code Civil, seules applicables en matière de cession de droit à l'image […] relèvent de la liberté contractuelle* ». Par conséquent, même si la Cour place le droit à l'image dans l'article 9 du Code Civil, relatif au droit au respect de la vie privée, le consentement reste le seul élément fondateur de licéité. Si celui-ci n'est pas vicié, la convention est valable, comme en l'espèce.

203. Dans un tel contexte, le risque d'une dépossession de la faculté de protéger sa vie privée est important pour l'utilisateur moyen. Au contraire de l'exploitation du droit à l'image que l'individu n'est pas forcé de brader, l'inscription sur le moindre service numérique nécessite l'acceptation d'un contrat ou d'une série de textes relatifs à la gestion des données. Mais pour comprendre les risques engendrés par une telle objectivisation il faut définir avec précision les critères de licéité du consentement dans le régime applicable aux données à caractère personnel, problématique abordée en deuxième partie.

426 Cass. Civ., 11 décembre 2008, n°07-19494, Bull. Civ. 2008, I, n°282.

Conclusion

204. La réduction du concept de vie privée entraine des conséquences importantes en termes de définition du périmètre de protection de l'individu face à l'innovation numérique. D'une part, les aspects sociaux manquants laissent se développer en dehors de toute possibilité d'analyse juridique un phénomène de bulle filtre qui va influencer les citoyens et les forces de l'ordre jusque dans la manière de penser ou d'engager leurs actions. D'autre part, la manière dont le droit s'est formé reflète une certaine complaisance vis-à-vis de la patrimonialisation des données. Dans un environnement où le consentement initial devient obligatoire avant d'accéder au moindre service, les obstacles à l'exploitation abusive qu'offrait le concept étendu de vie privée semblent impuissantes.

205. La protection qu'offre le régime ne donne pas un véritable pouvoir au citoyen, et ne le protège pas suffisamment vis-à-vis des nouveaux risques engendrés par le numérique. Bien au contraire, le régime entraine un phénomène d'accélération de la dépossession de la vie privée au profit des Etats et des organismes privés, en créant les conditions d'une exploitation libérale et utilitariste des données. Toute sa philosophie au regard du droit au respect de la vie privée peut finalement se résumer à un extrait de l'article 1 de la loi informatique et libertés : « *toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi* »[427]. Il ne s'agit donc pas d'un droit dont dispose véritablement la personne concernée, mais d'un périmètre décisionnel restreint que le législateur décide de lui laisser dans l'environnement numérique.

206. Enfin, à ces défauts majeurs du régime, s'ajoute également celui de la difficulté d'appréhender un phénomène technologique en mutation constante.

427 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, modifiée par la Loi n°2016-1321 du 7 octobre 2016 *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1, article 11.

Titre II

L'applicabilité du droit dans un contexte technologique mouvant

*

207. Le droit au respect de la vie privée ne peut se concevoir sans prise en compte de l'environnement technologique. La genèse de la loi informatique et libertés s'inscrit dans un tel contexte et se définit comme une réponse face à ce l'on appelait alors, « *les informations nominatives* »[428] et les atteintes du droit au respect de la vie privée que les traitements informatiques avaient la capacité de générer. Aujourd'hui, le nouveau règlement Européen[429] et les nombreuses législations[430] dont se dotent les Etats membres correspondent à une évolution des techniques de collectes et de traitements de l'information avec le développement du « *Big Data* ». Pour cette raison, toute analyse portant sur le droit au respect de la vie privée doit être nécessairement contextualisée à l'environnement technologique qui lui est contemporain, afin de vérifier si celui-ci est toujours adapté.

428 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, article 4.

429Règlement (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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

430 En France, on peut nommer la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016 ; la Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

208. Cette approche technologique peut toutefois avoir le défaut de réduire une atteinte à la vie privée à sa dimension purement technique, notamment en propageant la croyance répandue selon laquelle l'affaire SAFARI[431] constitue le premier exemple d'un traitement d'informations litigieux ayant donné lieu à une réponse législative. À cette primauté, l'affaire des fiches de 1904 reste la meilleure candidate[432]. Dès 1900, les loges maçonniques du Grand Orient de France avaient mis en place un système de fichage politique des militaires Français, ayant pour but de faciliter l'ascension des sympathisants de leur cause. Disposant d'un réseau étendu, les loges arrivaient à collecter et à traiter un grand nombre d'informations pendant près de quatre ans avant que le procédé soit dénoncé[433]. Le scandale eut des répercussions importantes sur les débats entourant la loi sur la séparation de l'Eglise et de l'Etat[434], mais plus encore, engendra l'intégration de l'article 65 dans la loi du 22 avril 1905[435]. Selon celui-ci : « *Tous les fonctionnaires civils et militaires, tous les employés et ouvriers de toutes administrations publiques ont droit à la communication personnelle et confidentielle de toutes les notes, feuilles signalétiques et tous autres documents composant leur dossier, soit avant d'être l'objet d'une mesure disciplinaire ou d'un déplacement d'office, soit avant d'être retardé dans leur avancement à l'ancienneté* » [436]. Il s'agit du premier exemple de droit d'accès à l'information par les personnes concernées.

209. À la lumière de cette affaire, on pourrait penser que la technologie n'introduit qu'un changement de moyens dans la gestion des informations, à défaut d'une transformation de la nature du procédé. Si dans l'exemple précédant, les capacités de traitement étaient liées au nombre d'individus et à l'étendue du réseau maçonnique, ceux-ci sont simplement remplacés par des algorithmes. Le droit n'aurait donc qu'à qualifier la nature de ce type d'atteintes, et non ses moyens. L'évolution technique importerait peu puisque la nature du procédé, jugé

431 Boucher Philippe, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.

432 v. Vindé Francois*, L'Affaire des Fiches, 1900-1904 : Chronique d'un Scandale*, Editions Universitaires, 22 décembre 1989, 236 p. ; Thuillier Guy, *Morale et Politique : Péguy et l'Affaire des Fiches en 1905*, La Revue administrative, 43e Année, n°256, Juillet-Août 1990, pp. 310-316 ; Charlot Patrick, *Péguy contre Jaurès : L'Affaire des Fiches et la Délation aux Droits de l'Homme*, Revue Française d'histoire des idées politiques, n°17, 1 semestre 2003, pp. 73-91.

433 Mayeur Jean-Marie, *La Vie Politique sous la Troisième République (1870-1940),* Seuil, 1 avril 1984, p. 190.

434 Loi du 9 décembre 1905, *concernant la séparation des Eglises et de l'Etat*, JORF du 11 décembre 1905, p. 7205.

435 Loi du 22 avril 1905, *portant fixation du budget des dépenses et des recettes de l'exercice 1905*, Recueil Duvergier, p. 268.

436 Ibid, article 65.

licite ou non, reste inchangée. Mais une telle approche minimise grandement le changement de paradigme qu'entrainement les systèmes de traitement automatisé de données.

210. Autrefois fastidieuses, les opérations de recensement nécessitaient la mobilisation de centaines de fonctionnaires pour compiler les différents rapports de leurs enquêteurs. S'inspirant des techniques de « *photo par perforation* » [437], Herman Hollerith mit au point une machine capable de lire des cartes perforées et améliora grandement les processus de comptage et de statistiques[438]. Bien que décisive dans la capacité d'un Etat à se renseigner sur ses administrés, le législateur ne perçut pas l'augmentation exponentielle du potentiel d'atteinte à la vie privée qu'impliquait cette innovation. Devenant plus tard International Business Machine (IBM), la société équipa la plupart des administrations de l'époque, devenant l'une des innovations prisées par le régime Nazi pour les recherches sur la filiation de ses citoyens et pour les procédures de gestion de ses camps d'extermination[439]. Il faudra attendre 1951, avec la loi sur l'obligation, la coordination et le secret en matière de statistique pour qu'un cadre strict viennent régir son utilisation[440]. On pourrait ainsi déplorer que le législateur n'ait pas souhaité intégrer dans son analyse sur la dangerosité du fichage des individus en 1905 les possibilités offertes par les premiers systèmes de traitement automatisé de l'information qui apparaissaient au même moment[441].

211. Une approche détachée du contexte technologique ne saurait saisir les risques réels qui pèsent sur la vie privée. De même, une approche purement technique n'aurait pas le recul suffisant pour juger de la pertinence à introduire une nouvelle législation. Il faut donc procéder à une analyse phénoménologique, replaçant le droit dans son contexte technologique, sans le lier à celui-ci. Dans cette perspective, le développement récent de technologie innovante introduit de nouveau un changement de paradigme.

437 Procédé technique observé à la fin du 19eme siècle, qui consiste en l'élaboration d'une fiche descriptive sur laquelle un opérateur perce les cases correspondantes à la description d'une personne (1.80m, cheveux bruns, etc.).

438 v. Hollerith Herman, *The Electrical Tabulating Machine,* Journal of the Royal Statistical Society, Vol. 57, n°4, December 1894, pp. 678-689.

439 v. Black Edwin, *IBM et l'Holocauste, l'Alliance Stratégique entre l'Allemagne Nazie et la Plus Puissante Multinationale Américaine*, Robert Laffont, 13 février 2001, 610 p. ; Gandillot Thierry, *Holocauste : Les listes IBM,* L'express, 15 février 2001, disponible sur http://www.lexpress.fr/informations/holocauste-les-listes-ibm_641323.html (consulté le 01/09/17).

440 Loi n°51-711 du 7 juin 1951, *sur l'obligation, la coordination et le secret en matière de statistiques*, JORF du 8 juin 1951, p. 6013.

441 Lee John A. N., *International Biographical Dictionary of Computer Pioneers*, Taylor & Francis, 1 novembre 1995, p. 378.

212. Si l'apparition des premières machines de traitement statistiques a constitué une rupture technologique, l'évolution ces dernières années des capacités de collectes et de traitement des informations est porteuse de nouveaux risques avec ce que l'on nomme : le « *Big Data* ». Ainsi que l'expliquent Kenneth Cukier et Viktor Mayer-Schoenberger, « *au départ, le concept a indiqué qu'à cause d'un volume d'informations devenu énorme, les capacités-mémoire des ordinateurs pour effectuer leur traitement étaient dépassées, et les ingénieurs devaient modifier les outils utilisés pour les analyser dans leur totalité. C'est là l'origine de nouvelles technologies de traitement de données comme MapReduce de Google, et son équivalent en version open source, Hadoop, créé sous l'impulsion de Yahoo. Elles permettent de gérer de bien plus grandes quantités de données qu'auparavant et – point important – il n'est pas besoin de ranger ces dernières de façon bien ordonnée ou dans des tables de base de données classiques. A l'horizon, se profilent de nouvelles technologies d'analyse de volumes considérables de données qui se passent de hiérarchies rigides et de l'homogénéité d'antan* » [442].

213. Face à cette nouvelle rupture technologique, dans un monde où l'affaire Snowden a révélé aux citoyens que ceux-ci étaient plus surveillés que jamais[443], il est nécessaire de définir de quelle manière le droit au respect de la vie privée s'applique dans le contexte technologique qui est le nôtre et de vérifier si celui-ci est suffisant au regard des nouvelles possibilités d'atteintes à la vie privée (1). Cela permettra de constater le basculement dont est victime le régime de protection dans la société de l'information à travers le phénomène, à la fois nécessaire et dangereux, de sa réinterprétation technique (2).

442 Cukier Kenneth, Mayer-Schoenberger Viktor, *Big Data : La Révolution des Données est en Marche*, Robert Laffont, 20 février 2014, p. 18.

443 v. Greenwald Glenn, *Nulle Part où se Cacher*, JC Lattès, 14 mai 2014, 280 p.

Chapitre 1

Le régime applicable aux nouvelles possibilités d'atteinte à la vie privée

*

214. Le 6 juin 2013, le quotidien Américain The Guardian publiait la première partie de la longue série d'informations fournies par l'ancien analyste de la NSA, Edward Snowden, sur les agissements de l'agence relatifs à la captation numérique[444]. Ces documents, dont l'exploitation est toujours en cours, mettent en lumière une maitrise technologique et une capacité de captation et de traitement de données sans précédent, portée presque exclusivement par les technologies numériques. L'agence est capable de collecter des données sur quasiment l'ensemble des services informatiques mondiaux, et cela, quels que soient les technologies ou les terminaux utilisés. Aujourd'hui, les capacités de détournements par les servies étatiques sont tels qu'un simple poste de télévision peut être transformé en dispositif d'écoute[445]. Face à ces révélations, le Parlement Européen décida de créer un comité d'experts ayant pour objectif d'enquêter sur les éléments techniques, et d'analyser le cadre juridique qui s'impose à ce type d'interceptions[446].

444 Greenwald Glenn, *NSA Collecting Phone Records of Millions of Verizon Customers,* The Guardian, 6 juin 2013.
445 Wikileaks, *Vault 7*, 7 March 2017, disponible sur https://wikileaks.org/ciav7p1/ (consulté le 01/04/17).
446 Procédure 2013/2188(INI), Parlement Européen, 12 mars 2014.

215. Plus que ces révélations, c'est l'efficacité du droit à protéger la vie privée dans un environnement technologique qui est remise en question, non seulement de par l'ampleur des écoutes révélées, mais aussi par les agissements frauduleux des cybercriminels qui sont en forte hausse. En 2016, Yahoo annonce le plus important vol de données au monde[447]. Plus d'un milliard de comptes sont concernés, ce qui bat le précèdent record établi par le piratage des bases de données de MySpace, avec ses 427 millions de mots de passe[448]. Pourtant, s'il s'agit principalement d'adresses emails et de mots de passe qui peuvent être révoqués, certains piratages touchent des données sensibles. Ainsi, les données du site internet de rencontres Ashley Madison contenaient les préférences sexuelles de ses 32 millions d'adhérents[449]. Rendues accessible sur internet, les données servirent par la suite à certaines opérations de rançons, lorsque l'identité des utilisateurs n'était pas directement publiée[450].

216. Dès lors, au-delà de l'analyse technique qui s'impose afin de sécuriser les informations des citoyens Européen, c'est bien le rapport de force entre le droit et ces nouvelles possibilités d'atteinte à la vie privée qu'il faut évaluer. Il ne s'agit pas de savoir si les citoyens sont bien maîtres de leurs données, mais quelles sont les techniques d'interceptions qui peuvent être mises en œuvre à leur insu, et de quelle manière celles-ci sont encadrées ou sanctionnées. Dans ce contexte, il est important de définir l'efficacité de l'encadrement des procédures d'interceptions de données (1) par les services régaliens, clé de voute de la confiance que les utilisateurs peuvent avoir en la technologique. De même, il faut nécessairement analyser le régime applicable aux atteintes aux systèmes de traitements automatisés de données (2) lorsque celles-ci visent à obtenir des données personnelles de manière illicite.

447 Gavois Sébastien, *Yahoo annonce le vol de données de plus d'un milliard de compte*, Next Impact, 15 décembre 2016, disponible sur https://www.nextinpact.com/news/102530-yahoo-annonce-vol-donnees-plus-dun-milliard-comptes.htm (consulté le 01/09/17).

448 Le Monde.fr, *Les principaux vols de donnée personnelles depuis 2013*, Le Monde, 29 septembre 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html (consulté le 01/09/17).

449 Ibid.

450 Untersinger Martin, *Suicides, démission, chantage : les conséquences tragiques du piratage du site de rencontres Ashley Madison*, Le Monde, 10 décembre 2015, disponible sur http://www.lemonde.fr/pixels/article/2015/12/10/suicides-demission-chantage-les-consequences-tragiques-du-piratage-du-site-de-rencontres-ashley-madison_4828391_4408996.html (consulté le 01/09/17).

Section 1

L'encadrement relatif des procédures d'acquisition de données par les services régaliens

217. L'examen de la licéité d'une acquisition de données à caractère personnel d'un citoyen par les services régaliens révèle la complexité du régime de protection de la vie privée. En effet, une telle opération se situe au carrefour des dispositions relatives à la protection de la vie privée[451], à la protection du domicile[452], à la protection des données à caractère personnel[453] et à la protection du secret des correspondances[454]. Il faut donc avoir une approche au cas par cas, en définissant le type de technologie qui peut être utilisée, la personne chargée de sa mise en œuvre, la finalité et le type de lieu visé ainsi que le moment où la collecte a lieu.

218. Cependant, pour circonscrire le spectre de notre étude, il convient de distinguer les méthodes innovantes de collecte de données à distance et les accès physique utilisés lors des perquisitions. Si les premières nécessitent un véritable examen au regard des nouvelles capacités d'intrusion et de captation, les seconds correspondent à la saisie, plus classique, de supports physiques par les forces de l'ordre dans le cadre des enquêtes judiciaires.

219. De manière liminaire, on peut rappeler que ces dernières sont soumises au régime des réquisitions informatiques et font l'objet de dispositions expresses dans les articles 57-1 et 60-2 du code de procédure pénale, ainsi qu'aux articles 76-3 et 77-1-1 selon qu'il s'agisse respectivement, d'enquêtes de flagrances ou d'enquêtes préliminaires.

451 Article 9 du Code Civil ; Article 226-1 et suivant du Code Pénal.
452 Article 226-4 du Code Pénal.
453 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227.
454 Article 226-15 du Code Pénal.

220. L'article 57-1 du code de procédure pénale autorise les officiers de police judiciaire, lors d'une perquisition, à « *accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Par extension, cette faculté reste licite si le système informatique saisi est déplacé dans les locaux d'une unité de police ou de gendarmerie. De la même manière, afin de répondre aux problématiques du stockage de données à l'étranger, la loi du 13 novembre 2014 autorise les forces de l'ordre à recueillir, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur, les données stockées à l'étranger mais accessibles à partir du système informatique initial[455]. Enfin, selon l'article 77-1-1 du code de procédure pénale, si ces procédures sont engagées dans le cadre d'une enquête préliminaire, les réquisitions doivent être autorisées par le procureur de la république ou par l'officier de police judiciaire sous peine de nullité[456].

221. Si ces procédés restent similaires à ceux utilisés pour les objets usuels dans le cadre d'une enquête judiciaire, nous pouvons constater des évolutions récentes dans les textes ayant traits aux interceptions numérique qui accroissent le pouvoir des services étatiques dans le numérique. À titre d'exemple, la modification des dispositions du code de procédure pénale relatives au recueil d'informations en provenance de services tiers par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé a tenu compte de l'évolution des moyens technologiques[457]. Selon le nouvel article 60-1 du CPP : « *le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privée ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel* ». Cela s'applique particulièrement aux fournisseurs d'accès, directement visés par l'article 60-2 du Code de procédure pénale, avec l'obligation de fournir à la demande des autorités les informations de connexion de leurs

455 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, p. 19162

456 Cass. Crim., 1 septembre 2005, n°05-84.061, Bull. Crim. n°139, D. 2006, p. 2836.

457 Loi n°2016-737 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, texte n°1.

clients. Or, ces derniers ont un rôle particulièrement central dans l'accès à internet. À la lumière de ces évolutions législatives, il convient de définir avec précision quels sont les moyens à la disposition des forces régaliennes pour recueillir des informations numériques dans la société de l'information.

222. Les services régaliens ne disposent pas des mêmes accès aux données selon les cas d'espèce. Ces moyens correspondent à l'étendue des pouvoirs d'enquêtes attribués aux différents services en fonction de la nature des infractions. Le régime des interceptions informatiques est lié à celui des interceptions des correspondances fondé par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[458] et conserve la distinction existante entre le régime de droit pénal commun (les interceptions judiciaires) et celui applicable en matière de défense des intérêts de l'Etat (les interceptions administratives). Les dispositions législatives et réglementaires afférentes se trouvent respectivement dans le code de procédure pénale et dans le code de la sécurité intérieure. Pour les premières, il s'agit essentiellement d'un pouvoir de collecte des données des tiers pour les besoins d'enquête, avant que la loi du 3 juin 2016 les dote de nouveaux moyens numériques d'intrusion dans les systèmes de traitements automatisés de donnée[459]. Pour les secondes, il s'agit des pouvoirs de captation ou d'intrusion des services de renseignement qui s'étaient développés, de l'aveu même du rapport d'information sur le projet de loi renseignement, « *en l'absence d'un cadre juridique global et cohérent définissant ses finalités, ses acteurs, leurs moyens d'intervention et les modalités de son contrôle* » [460], avant que la loi du 24 juillet 2015 relative au renseignement ne vienne compléter ces dispositions[461].

458 Loi n°91-646 du 10 juillet 1991, *relative au secret des correspondances émises par la voie des télécommunications*, JORF n° 106 du 13 juillet 1991, p. 9167.

459 Loi n°2016-737 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, texte n°1.

460 Bas Philippe, *Rapport n°460 fait au nom de la commission des lois, au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale, sur le projet de loi, adopté par l'Assemblée nationale, après engagement de la procédure accélérée, relatif au renseignement et, sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, Déposé à l'Assemblée Nationale le 20 mai 2015, p. 12.

461 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

223. L'étendue de ce maillage de collecte de données est pourtant difficile à définir dans un environnement où les services informatiques ont une place centrale dans la façon dont les internautes s'informent ou échangent des informations. Aux Etats Unis par exemple, les documents fournis par Edward Snowden, ont montré qu'une grande partie de ces collectes étaient réalisées de manière systématique et transnationale[462], remettant en question l'efficacité des mesures de protection de la vie privée numérique. Dès lors, il convient de définir le périmètre de captation licite de données dans lequel les autorités peuvent collecter des informations sur les citoyens selon qu'il s'agisse d'interceptions judiciaires (1) ou administratives (2).

1 – Le périmètre de collecte des interceptions judiciaires

224. Le pouvoir de collecte des interceptions judiciaires, hormis le régime applicable aux perquisitions, consiste essentiellement à rassembler les données disponibles sur un individu, en requérant les informations dont disposent les organismes publics ou privés sur celui-ci en vertu de l'article 60-1 du code de procédure pénale. La justice s'appuie sur la mise en place d'un système de transmission d'interceptions judiciaire, par le décret du 30 juillet 2007, afin de constituer une plateforme nationale facilitant le travail d'enquête[463]. Ce système peut être utilisé par les magistrats qui prescrivent ou requièrent les interceptions judiciaires, les officiers de police judiciaire chargés de les seconder ainsi que les agents des douanes habilités. Son accès est contrôlé par un magistrat du siège hors hiérarchie, nommé pour trois ans par arrêté du garde des sceaux, et assisté par trois membres nommés dans les mêmes conditions. Chaque consultation est enregistrée, et liée à l'identifiant de l'agent ayant eu accès aux fichiers[464].

225. Selon son article 2 : « *la finalité de ce traitement est de mettre à la disposition des magistrats, officiers de police judiciaire et agents des douanes habilités à effectuer des enquêtes judiciaires, qui procèdent (…) à des interceptions de correspondances émises par la*

462 À titre d'exemple, v. Greenwald Glenn, *NSA Collecting Phone Records of Millions of Verizon Customers,* The Guardian, 6 juin 2013.

463 Décret n°2007-1145 du 30 juillet 2007 *portant création d'un traitement automatisé de données à caractère personnel dénommé "système de transmission d'interception judiciaires"*, JORF n°175 du 31 juillet 2007, p. 12862, texte n°23.

464 Décret n°2007-1145 du 30 juillet 2007 portant création d'un traitement automatisé de données à caractère personnel dénommé "système de transmission d'interception judiciaires", JORF n°175 du 31 juillet 2007, p12862, texte n°23, article 4.

voie de communications électroniques, les données relatives au trafic et le contenu des minimessages émis ou reçus par un numéro de téléphone dont la ligne est interceptée et qui leur sont transmis par les opérateurs de communications électroniques. Les données relatives au trafic des interceptions et le contenu des minimessages font l'objet d'un chiffrement » [465]. Concrètement, lorsqu'un agent habilité souhaite collecter les données d'un individu, la plateforme gère automatiquement la demande auprès du fournisseur d'accès, qui lui envoie les données demandées. La plateforme transmet les métadonnées[466] dont les fournisseurs d'accès doivent garder une trace pendant une année, d'abord en vertu de la directive 2002/58[467], puis en conformité avec la loi du 21 juin 2004 pour la confiance dans l'économie numérique[468] et du décret du 25 février 2011 qui fixe l'étendu des données concernées par cette mesure[469].

226. Celles-ci sont exploitables indifféremment, qu'il s'agisse d'un accès téléphonique ou d'un accès internet. Dans l'article 4 du décret portant création du système de transmission d'interception judiciaire sont évoquées expressément : « *les données relatives au trafic des interceptions comportent, pour chaque communication, notamment l'indication du code de l'opérateur, des numéros de téléphone, des adresses de messageries des appels et des appelants, de la date, l'heure, la durée de l'appel et l'identification des connexions activées* »[470]. Cependant, l'article 1 du décret du 25 février 2011 établit une liste qui s'applique d'avantage aux fournisseurs de connexion internet comprenant : « *l'identifiant de connexion, l'identifiant attribué par ces personne à l'abonné, l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès, les dates et heure de début et de fin de la connexion, les caractéristique de la ligne de l'abonné* » [471]. Par ailleurs, les minimessages

465 Ibid.

466 Ensemble structure de données qui, pour une communication, peuvent déterminer l'identité de l'émetteur et du récepteur, le temps ou la taille des données échangées, ainsi que les dates des échanges, sans indiquer le contenu précis de la communication.

467 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

468 Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2, article 6.

469 Décret n°2011-219 du 25 février 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, JORF n°0050 du 1 mars 2011, p. 3643, texte n°32.

470 Décret n°2007-1145 du 30 juillet 2007 *portant création d'un traitement automatisé de données à caractère personnel dénommé "système de transmission d'interception judiciaires"*, JORF n°175 du 31 juillet 2007, p. 12862, texte n°23.

471 Décret n°2011-219 du 25 février 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, JORF n°0050

sont conservés par le système de transmission d'interceptions judiciaires jusqu'à leur réception, et effacés trente jours après leur envoi. Les métadonnées, quant à elles, sont conservées 3 ans par le système. Il y a donc deux durées de conservation différentes, un an par les opérateurs réseaux et trois ans par le système d'interception judiciaire.

227. Le périmètre exact de captation reste dépendant de la qualification des organismes visés par ces mesures. S'il existait un doute à leur encontre, la récente proposition de modification de la directive 2002/58 par la Commission Européenne indique dans son article 11 que les services de messageries numériques ou les réseaux sociaux, n'étant pas eux même fournisseurs de réseaux, sont aussi visés, en supprimant la distinction qui existait entre fournisseur d'accès et service numériques. Réunis dans une même définition: « *les fournisseurs de services de communications électroniques devront établir des procédures interne afin de répondre aux requêtes d'accès aux données de leurs utilisateurs basées sur des exigences législatives* »[472]. Dès lors, on peut supposer qu'il existera, d'ici peu de temps sur le territoire Français, un système informatisé d'accès à l'ensemble des métadonnées de télécommunications des citoyens, quel que soit le moyen de télécommunication physique ou numérique, par les services de police et de gendarmerie.

228. Toutefois, son périmètre pourrait se voir réduit par la récente décision de la Cour de Justice Européenne. Dans son arrêt du 21 décembre 2016, celle-ci énonce que la directive 2002/58 modifiées par la directive 2009/136, « *lu à la lumière des articles 7,8,9 et 11, ainsi que l'article 52 paragraphe 1 de la charte des droits fondamentaux de l'Union Européenne, doit être interprété en ce sens (qu'elle) s'oppose à une réglementation nationale prévoyant à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* » [473]. Selon le rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année

---

du 1 mars 2011, p. 3643, texte n°32.

472 Traduction par l'auteur de: « *Providers of electronic communications services shall establish internal procedures for responding to requests for access end-users' electronic communication data based on a legislative measure* ». Commission Européenne, *Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/CE (Regulation on Privacy and Electronic Communications)*, COM/2017/10 Final, Brussels, 10 January 2017.

473 CJUE gr. ch., 21 décembre 2016, Tele2 Sverige AB c. Post-och Telestyrelsen, aff. jtes. C-203/15 et C-698/15.

2016 : « *l'arrêt ne remet pas en cause l'accès des juges ou des services de renseignement au fadettes, mais il censure leur conservation, en tout cas pour une période dépassant un délai très bref. Il n'autorise plus, au fond, que les récupérations de données de connexion effectuées en temps réel* » [474].

229. Cette décision intervient alors même que la directive relative à l'échange entre les autorités des Etats membres d'informations portant sur la prévention ou la détection des infractions vient d'entrer en vigueur[475]. Cependant, on peut faire un rapprochement avec la logique du Conseil Constitutionnel lors de l'examen de la loi renseignement intervenu quelques semaines plus tôt. En l'espèce, plusieurs associations de défense de la vie privée avaient déposé une question prioritaire de constitutionnalité face à l'autorisation de collecte et de traitement des transmissions empruntant la voie hertzienne, sans dispositif de contrôle, dans la proposition de loi sur le renseignement de 2015[476]. Constatant que « *les dispositions contestées ne définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre (et) qu'elles ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie* »[477], les sages censurèrent la disposition incriminée pour atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances.

230. On peut penser que le régime autorisant l'enregistrement systématique des métadonnées des citoyens Français sur les réseaux de télécommunication par les fournisseurs d'accès puisse souffrir d'un manque de légalité lié à son caractère systématique, alors même que le dispositif est au centre du régime applicable aux interceptions judiciaires. Cependant, cela ne semble pas concerner les dispositions de la loi du 3 juin 2016 relative aux interceptions.

474 Adam Patricia, *Rapport n° 4573 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, Enregistré à la Présidence de l'Assemblée Nationale le 2 mars 2017, p. 80.

475 Directive 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement de 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/JAII du Conseil, JOUE, 4 mai 2016, L 119/89.

476 Projet de loi relative au renseignement, n°2669, enregistré à la Présidence de l'Assemblée Nationale le 19 mars 2015.

477 Conseil Constitutionnel, Décision n°2016-590-QPC du 21 octobre 2016, *La Quadrature du Net et autres*, Journal officiel n°0248 du 23 octobre 2016, texte n°37.

231. Initialement prévue par la loi d'orientation et de programmation pour la performance de la sécurité intérieure[478], puis largement remanié par la loi du 3 juin 2016[479], le régime applicable aux interceptions judiciaires vise les infractions prévues à l'article 706-73 et 707-73-1 du code de procédure pénale. Il s'agit principalement d'infractions commises en bande organisée et autres délits aggravés de traite des êtres humains, de proxénétisme, de terrorisme ou d'atteinte aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat. Pour ces délits et en dehors de l'autorisation d'exploitation du système de transmission d'interceptions judiciaires, les nouveaux articles 706-102-1 et 706-102-2 du code de procédure pénal autorise le juge des libertés et de la détention et le juge d'instruction, respectivement à la requête ou après l'avis du procureur de la République, à « *autoriser par ordonnance motivée les officiers et agents de police judiciaire (…) à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur (…), telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels* ». De plus, le procureur de la République peut designer certains experts pour réaliser ces intrusions, ainsi que recourir aux moyens de l'Etat soumis au secret de la défense nationale.

232. Ces dispositions autorisent l'usage de logiciels d'intrusions informatiques dans les systèmes de traitement de données, qui peuvent être assimilées à des technologies de piratage. Ces technologies, produites en grande partie par des sociétés privées, s'appuient sur la découverte de faille dans les différents logiciels et autres systèmes d'exploitation. Les experts nomment cela, de la « *sécurité offensive* »[480], et ces techniques sont utilisées par les principaux services étatiques à travers le monde[481], notamment dans le cadre des interceptions administratives.

478 Loi n° 2011-267 du 14 mars 2011, *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n°0062 du 15 mars 2011, p. 4582, texte n°2.

479 Loi n°2016-737 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, texte n°1.

480 Eudes Yves, *Hackers d'Etat, Enquête sur ces sociétés de sécurité offensive spécialisées dans la découverte de failles informatiques, qui vendent leurs trouvailles à des organismes officiels*, Le Monde, 19 février 2013, disponible sur http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html (consulté le 01/09/17). .

481 v. Vault 7 Project, site internet de Wikileaks, disponible sur https://wikileaks.org/vault7/ (consulté le 01/09/17).

2 – Le périmètre de collecte des interceptions administratives

233. En 2015, un rapport d'information considérait que « *l'absence d'un corpus juridique encadrant l'activité des services de renseignement expose notre pays à des risques non négligeables de condamnation par la Cour Européenne des droits de l'Homme* » [482]. De son côté, le centre de recherche de l'école des officiers de la Gendarmerie Nationale jugeait que « *la légitimité du renseignement exige une loi précise, pour ne pas encourir le grief d'incompétence négative, prévisible dans ses conséquences, accessibles à tous, et qui, par ses finalités et les moyens mis en œuvre réponde à un besoin social impérieux, à une nécessité d'intérêt public, et respecte le principe de proportionnalité* » [483]. C'est dans ce contexte que fut introduite la proposition de loi sur le renseignement en mars 2015, cherchant à concilier l'exigence d'une certaine transparence et un renforcement du droit au respect de la vie privée avec les objectifs de sécurité[484].

234. Celle-ci proposait des changements importants dans le code de sécurité intérieure, en légitimant une série de mesures techniques relatives à l'élargissement des capacités administratives de captation et d'interception de données. La première de celles-ci, est l'installation de « *boites noires* »[485] sur les réseaux des opérateurs de communication électroniques et des différents services de l'innovation numériques, afin de collecter les informations et les documents traités par le réseau. La seconde, consiste en la mise en place obligatoire, aux seuls besoins de la prévention du terrorisme, d'un algorithme de détection des connexions et de comportements susceptibles de révéler une menace terroriste. Enfin, une série de mesures étend les capacités de collectes d'informations et de localisation aux personnes en relation avec un individu initialement repéré. En échange de cette dotation

482 Bas Philippe, *Rapport n°460 fait au nom de la commission des lois, au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale, sur le projet de loi, adopté par l'Assemblée nationale, après engagement de la procédure accélérée, relatif au renseignement et, sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, Déposé à l'Assemblée Nationale le 20 mai 2015, p. 24.

483 Centre de recherche de l'école des officiers de la Gendarmerie Nationale, Note numéro 13, Septembre 2015, p. 1.

484 Projet de loi relative au renseignement, n°2669, enregistré à la Présidence de l'Assemblée Nationale le 19 mars 2015.

485 Système informatique de collecte et de traitement d'informations, dont le fonctionnement interne est inconnu du service qui l'héberge.

technique, la proposition de loi remplace la Commission nationale de contrôle des interceptions de sécurité, créée par la loi du 10 juillet 1991[486], par la Commission nationale de contrôle des techniques de renseignement, et place la procédure d'autorisation de mise en œuvre des collectes sous l'autorité du premier ministre. De plus, elle fixe une durée maximale de la conservation des informations en fonction des différentes technologies.

235. Consultée sur la portée du texte, la CNIL va souligner dans son avis du 5 mars 2015 le fait que « *si toutes ces techniques ne revêtent pas la même sensibilité du point de vue du respect de la vie privée, l'ensemble des dispositions ainsi projetées permettra la mise en œuvre de mesures de surveillance beaucoup plus larges et intrusives que ce qu'autorise le cadre juridique actuel en matière de renseignement. En effet, parmi les nouvelles techniques de recueil du renseignement légalisées ou autorisées, certaines sont susceptibles de conduire à une surveillance massive et indifférenciée des personnes* »[487]. Elle émettra, en conséquence, un avis largement défavorable. Fait rare, afin d'éviter toute polémique, le Président de la République saisira directement le Conseil Constitutionnel afin d'obtenir son avis préalablement à la promulgation du texte. Celui-ci, dans sa décision datée du 23 juillet 2015, validera en grande partie les dispositions techniques, en rappelant le caractère exclusivement administratif de ces mesures : « *le recueil de renseignement au moyen des techniques définies par la loi relève de la seule police administrative. Il ne peut ainsi avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions. Il ne peut être mise en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs* »[488]. Validée en majeure partie, la loi sera promulguée le 15 juillet 2015[489].

236. En fonction des différentes techniques ou des circonstances de l'espèce, les services administratifs seront en mesure de capter un nombre d'informations supérieur à celui dont dispose les services judiciaires en matière pénale. Intégrées aux articles L851-1 et suivants du code de la sécurité intérieure, ces technologies de collecte et d'analyse systématique des réseaux de télécommunications sont en grande partie réservées au cas d'entreprises terroristes.

486 Loi n°91-646 du 10 juillet 1991, *relative au secret des correspondances émises par la voie des télécommunications*, JORF n° 106 du 13 juillet 1991, p. 9167.

487 Commission Nationale de l'Informatique et des Libertés, Délibération n°2015-078 du 5 mars *2015 portant avis sur un projet de loi relative au renseignement*, Publiée sur Légifrance le 25 mars 2015.

488 Conseil Constitutionnel, Décision n°2015-713 du 23 juillet 2015, *Loi relative au renseignement*, Journal officiel n°0171 du 26 juillet 2015, p. 12751, texte n°4.

489 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

Cependant, la nouvelle formulation de l'article L 811-3 du code de la sécurité intérieure introduit une certaine ambiguïté, en autorisant par une formule généraliste le recours à ces techniques dans un champ qui couvre : « *l'indépendance nationale, l'intégrité du territoire et la défense nationale ; les intérêts majeurs de la politique étrangère ; l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; les intérêt économiques, industriels et scientifiques majeurs de la France ; la prévention du terrorisme ; la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, des violences collectives de nature à porter gravement atteinte à la paix publique ; la prévention de la criminalité et de la délinquance organisée ; la prévention de la prolifération des armes de destruction massive* » [490].

237. De plus, cette nouvelle loi crée les articles L853-2 et 853-3 du code de la sécurité intérieure relatifs aux techniques d'accès aux données informatiques stockées dans les systèmes informatiques tiers. De la même manière que pour les services judiciaires, le personnel habilité pourra « *accéder à des données informatiques, les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels* » [491]. Cependant, si précédemment les interceptions judiciaires étaient limitées par le cadre strict d'une enquête, la formulation de l'article L811-3 autorise l'utilisation de ces technologies pour une large palette de motifs.

490 Article L 811-3 du code de la sécurité intérieure
491 Article L853-2 du code de la sécurité intérieure

Conclusion

238. L'examen des documents de Snowden par Glenn Greenwald montrait qu'il existait, aux Etats-Unis, une main mise technologique de la NSA sur l'ensemble des réseaux informatiques, ainsi que des capacités d'intrusions extrêmement sophistiquées[492]. En France, bien que peu de détails techniques filtrent sur les méthodes existantes, les interceptions judiciaires bénéficient d'outils similaires, avec un système automatique de traitement des demandes d'interceptions judiciaires ciblant les métadonnées des fournisseurs de réseaux et de service, et des technologies d'intrusions pouvant aller jusqu'à recourir aux moyens de l'Etat protégés par le secret défense pour collecter les données des suspects. Cependant, leur utilisation reste réduite à la dimension de l'enquête et soumise au contrôle du juge d'instruction ou du procureur de la République selon le fondement de l'action pénale. Dès lors, on peut considérer que dans le cadre judiciaire, l'usage de ces technologies est intimement lié à la qualification pénale de l'infraction initiale, qui déterminera ensuite la licéité d'un recours aux technologies les plus intrusives selon son affinité avec les délits définis dans les articles 706-73 et 707-73-1 du code de procédure pénale. Au-delà de l'action protectrice des instances de contrôle, c'est le système juridique pénal lui-même qui garantit l'encadrement strict de l'utilisation de ces technologies avec la sanction de nullité qui vient frapper tout manquement.

239. Ce double système de protection, structurel par la place accordée au juge d'instruction et au procureur de la République, et systémique par son ancrage dans le code de procédure pénale, semble offrir aux citoyens Français un cadre suffisamment strict pour limiter les utilisations régaliennes frauduleuses, à l'inverse du régime applicable aux interceptions administratives.

240. Ayant accès aux mêmes types de technologies de collecte et d'intrusion, les services d'interceptions administratives bénéficient en plus de la récente légalisation des méthodes de collectes algorithmiques systématiques, avec l'obligation pour les fournisseurs d'accès d'installer des « *boites noires* » au cœur de leurs systèmes[493]. Ils disposent d'un accès direct

492 v. Untersinger Martin, *En trois ans, qu'a-t-on appris des documents Snowden ?,* Le Monde, 17 décembre 2016.

493 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735,

aux informations de connexion et autres métadonnées, sans qu'une action du fournisseur de réseau soit requise. De plus, on peut noter que l'examen de la proportionnalité d'une mesure de surveillance par la Commission Nationale de Contrôle des Techniques de Renseignements ne se fait plus sur la base d'une demande d'interception de ligne, mais d'une demande d'interception de cible[494], pouvant également s'étendre à ses proches[495]. Enfin, bien que soumise à autorisation du Premier Ministre après avis de la CNTCR, la mise en œuvre de ces moyens techniques peut être justifiée dans le large spectre couvert par l'article L 811-3 du code de la sécurité intérieure[496].

241. À la différence des interceptions judiciaires, l'ensemble du contrôle de la mise en œuvre de ces technologies massives et intrusives repose essentiellement sur l'appréciation de la CNCTR. La Commission est dotée d'un double rôle, émettre un premier avis a priori, et contrôler l'exécution des mesures de surveillance a posteriori. Toutefois, le recours au code de la sécurité intérieure et la large définition des finalités acceptables de l'article L.811-3 lui laisse une faible marge d'appréciation. Cela se traduit par les chiffres impressionnants du nombres d'avis préalables rendus en la matière, exprimés dans le premier rapport d'exercice de la Commission, avec 48 208 avis concernant l'accès aux données de connexions en temps différé, 2127 pour la géolocalisation en temps réel, 8538 interceptions de sécurité, et 7711 autres techniques non détaillées entre 2015 et 2016[497].

242. On peut considérer qu'en l'état actuel de la législation, un détournement des nouvelles possibilités offertes par les technologies de traitement de données est réalisable à travers l'utilisation abusive des procédures d'interceptions administratives. Ces technologies de surveillance, intégrées au cœur des réseaux, sont d'ailleurs l'une des mesures les plus

texte n°2.

494 Article L.821-2 du code de la sécurité intérieure.

495 Article L.852-1 du code de la sécurité intérieure

496 Article L.811-3 du code de la sécurité intérieure: «*Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignements peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil de renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nations suivant : l'indépendance nationale, l'intégrité du territoire et la défense nationale ; les intérêts majeurs de la politique étrangère ; l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; les intérêt économiques, industriels et scientifiques majeurs de la France ; la prévention du terrorisme ; la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, des violences collectives de nature à porter gravement atteinte à la paix publique ; la prévention de la criminalité et de la délinquance organisée ; la prévention de la prolifération des armes de destruction massive* ».

497 Commission Nationale de Contrôle des Techniques de Renseignement, *1er rapport d'activité 2015-2016*, p. 65.

étendues dans le cadre de l'Etat d'urgence par la loi 21 juillet 2016[498], en s'appliquant à toute personne « *susceptible d'être en lien avec une menace* » [499], et cela, en dehors de tout contrôle des juges. On ne peut que déplorer le sacrifice des barrières protectrices de la vie privée lié au virage sécuritaire que les forces régaliennes semblent opérer pour répondre aux problématiques de terrorisme. Dans un tel environnement législatif, l'émergence de technologies de sécurisation des informations à destination des citoyens est particulièrement opportune, pour que ces derniers puissent se protéger à la fois des velléités Etatiques et des malfaiteurs.

Section 2

Les insuffisances du régime applicable aux atteintes aux systèmes de traitement de données

243. Si les services étatiques suscitent une certaine crainte des citoyens vis à vis de la protection de la vie privée, les agissements frauduleux constituaient en 2016 une part non négligeable des atteintes aux données à caractère personnel[500]. Selon l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) : « *les intrusions informatiques destinées à dérober des informations personnelles (identité, données d'identification à des sites marchands, données bancaires) se multiplient. Il s'agit le plus souvent pour des criminels de commettre des délits identiques à ceux connus dans le monde matériel – vols, escroqueries, chantage -, mais de manière industrialisée, une part du risque d'être identifié et poursuivi en moins. (…) Ses capacités techniques sont croissantes au point d'être désormais en mesure de pratiquer, pour lui-même ou en sous-traitante par hybridation, des actes de sabotage ou de*

498 Loi n°2016-987 du 21 juillet 2016, *prorogeant l'application de la loi n°55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste*, JORF n°1069 du 22 juillet 2016, texte n°2.

499, Ibid, Article 15.

500 Le Monde.fr, *Les principaux vols de donnée personnelles depuis 2013*, Le Monde, 29 septembre 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html (consulté le 01/09/17).

244. *prise en otage d'outils de production* »[501]. Sur ce point, deux types d'infractions peuvent être constatées en ce qui concerne la protection des données à caractère personnel. Soit une entreprise crée ou détourne, de manière illicite, une collecte ou un traitement de données dont elle a la charge. Soit il s'agit d'une intrusion frauduleuse dans un système de traitement de données.

245. Sur le premier point, il nous faut rappeler qu'une personne morale ou physique est soumise au régime de la loi du 6 janvier 1978[502], dont les sanctions en cas de détournement de la finalité ou de collecte illicite sont décrites au point 156 de cet ouvrage, et n'appellent pas de commentaire particulier quant à l'application de celles-ci en cas de manquement. Cependant, l'intrusion dans un système de données constitue une infraction qui relève d'un régime différent. Ainsi, la loi Godfrain du 5 janvier 1988[503] a introduit dans le code Pénal une disposition qui, dans sa dernière version, tend à condamner le fait « *d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* »[504], qu'il puni de deux ans d'emprisonnement et de 30 000€ d'amende. Pourtant, ces mesures semblent peu dissuasives. Selon l'observatoire National de la Délinquance et des réponses pénales, les atteintes aux systèmes de traitements automatisés de données ont augmentées de 48,6% entre 2014 et 2015, avec une année 2015 qui totalise 9807 atteintes enregistrées par les services de police et les unités de gendarmerie nationale[505].

246. Dans ce contexte, on peut s'interroger sur l'efficacité des mesures pénales face aux atteintes aux systèmes d'information (1) ayant pour but d'obtenir des données à caractère personnel. À l'heure où de plus en plus d'internautes se tournent vers des solutions innovantes pour se rendre maîtres de leur protection, s'appropriant les technologies d'anonymisations et de sécurisations des données (2), la question de la place du droit face à la technologie semble ressurgir.

501 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, article 4.

502 Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI), *Stratégie nationale pour la sécurité du numérique*, 2015, p. 7.

503 Loi n°88-19 du 5 janvier 1988, *relative à la fraude informatique*, JORF du 6 janvier 1988, p. 231.

504 Code Pénal, article 323-1.

505 Observatoire National de la délinquance et des réponses pénales, *Rapport Annuel 2016 de l'ONDRP, La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet en 2015,* novembre 2016, p. 2.

1 – La répression des atteintes aux systèmes de traitement de données

247. Même si l'on peut différencier les types d'attaques informatiques selon le mode opératoire[506], la finalité reste l'accès au système. C'est sans doute sur la base de cette observation que la loi Godfrain du 5 janvier 1988 a regroupé l'ensemble de ces activités sous la dénomination d'accès ou de maintien frauduleux « *dans tout ou partie d'un système de traitement automatisé de données* » [507], et a introduit les articles 462-2 et suivants du code pénal pour ce type d'infraction. La loi pour la confiance dans l'économie numérique du 21 juin 2004[508] modifiera et déplacera l'ensemble de ces dispositions aux articles 323-1 et suivants, en créant un nouveau délit avec l'article 323-3-1 condamnant : « *le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute données conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 et 323-2* ». Néanmoins, la formulation est opportuniste en résistant au piège de définir avec précision les typologies d'intrusions frauduleuses, et laisse aux juges du fond l'appréciation de ce qui constitue un système de traitement automatisé de données et un accès frauduleux.

248. Ces derniers ont opté pour une appréciation large de la définition de système d'information. Un réseau bancaire[509], un disque dur[510] ou un radiotéléphone[511] sont considérés comme tels. Tout ensemble structuré de données constitue donc un système de traitement automatisé de données au sens des articles 323-1 et suivants du code pénal. Concernant la définition d'un accès frauduleux, la Cour d'Appel de Paris, dans son arrêt du 5 avril 1994, a considéré que « *l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà*

506 Loi n°88-19 du 5 janvier 1988, *relative à la fraude informatique*, JORF du 6 janvier 1988, p. 231.
507 v. Engebretson Patrick, *Les Bases du Hacking*, Pearson, 23 août 2013, 240 p.
508 Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2.
509 Trib. Corr. Paris, 13eme ch, 25 février 2000.
510 CA. Douai, 7 octobre 1992.
511 CA. Paris, 18 octobre 1992.

sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication » [512]. De plus, « *pour être punissable, cet accès ou ce maintien doit être fait sans droit et en plein connaissance de cause* » [513].

249. Selon cette définition, la notion d'accès frauduleux intègre nécessairement un caractère intentionnel. Or, certains systèmes peuvent être, volontairement ou accidentellement, accessibles à distances, sans que l'internaute puisse prendre la mesure juridique de l'action qui le conduit à y accéder. Dans l'affaire Tati, un journaliste spécialisé dans la dénonciation des insuffisances de protections des données a pu accéder à l'aide de son seul navigateur à des données à caractère personnel en provenance de la société Tati. La Cour d'Appel de Paris rejeta la qualification aux motifs « *qu'il ne peut être reproché à un internaute d'accéder, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection (...) devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès (...)* » [514]. Ce faisant, la Cour d'Appel opère un revirement de la responsabilité de l'intrusion, en faisant peser sur le responsable du site internet l'obligation de sécuriser les accès aux données. Cette obligation sécurisation, résultant de la loi informatique et libertés relative aux données à caractère personnel[515] a d'ailleurs été étendue à d'autres types d'infrastructures depuis, notamment pour les opérateurs d'importance vitale avec la loi de programmation militaire[516].

250. Par son arrêt du 20 mai 2015, la chambre criminelle de la Cour de Cassation rejette une telle analyse pour un cas d'espèce similaire, dans lequel une personne avait pu télécharger des documents sur un serveur distant en y accédant à partir d'une simple recherche sur le service Google Search[517]. Celle-ci, focalisant son analyse sur l'élément intentionnel de l'infraction, considère que « *le prévenu a parfaitement reconnu qu'après être arrivé par erreur au cœur de l'extranet de l'agence nationale de sécurité sanitaire de l'alimentation*

512 CA. Paris, 5 avril 1994, D. 1994, IR, p. 130.
513 Ibid.
514 CA. Paris, 12eme ch, 30 octobre 2002.
515 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227.
516 Loi n°2013-1168 du 18 décembre 2013, *relative à la programmation militaire pour les années 2014-2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, JORF n°0294 du 19 décembre 2013, p. 20570, texte n°1.
517 Cass. Crim., 20 mai 2015, pourvoi n°14-81336, Bull. Crim. 2015, n°119.

(ANSES), avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil, il avait constaté la présence de contrôle d'accès et la nécessité d'un authentification par identifiant et mot de passe ; qu'il est ainsi démontré qu'il avait conscience de son maintien irrégulier dans le système de traitement automatisé de données visitées ou il a réalisé des opération de téléchargement de données à l'évidence protégées »[518]. Par conséquent, la qualification d'accès frauduleux ne repose pas sur l'accès en soit, mais sur la qualification des éléments intentionnels factuels entourant cette intrusion.

251. Au cœur de ce régime de protection, les données sont directement visées par l'article 323-3 du code pénal, récemment modifié par la loi du 24 juillet 2015[519], punissant de cinq ans d'emprisonnement et de 150000 euro d'amende : le fait « *d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* ». Ces peines sont doublées lorsqu'il s'agit d'un traitement mis en œuvre par l'Etat. De plus, selon l'article 323-7, la simple tentative de ce type de délit est punie des mêmes peines. Enfin, il faut noter que ces peines sont cumulables avec les sanctions infligées par la CNIL, dont nous avons donné le détail au point 156 de cet ouvrage.

252. Sur la base de ce constat, il semble que l'applicabilité de la loi Godfrain relative aux accès frauduleux couvre avec suffisamment de clarté les infractions informatiques pour permettre une répression efficace par les tribunaux. Cependant, ces mesures, si claires soient elles, font face à une difficulté inhérente aux TIC : leur répartition géographique et les difficultés techniques liées à l'identification des auteurs d'infractions. En effet, pour déterminer l'identité d'un auteur d'infraction, il faut nécessairement obtenir la correspondance entre l'adresse IP relevée et l'identité de la personne détentrice de l'abonnement auprès du fournisseur d'accès à internet. Or, dans un grand nombre de cas, celui-ci se trouve à l'étranger.

253. Si l'auteur de l'infraction agit depuis un pays membre de l'Union Européenne, plusieurs dispositions existent pour faciliter les échanges d'informations. Successivement,

518 Ibid.

519 Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

l'ancienne directive 95/46/CE[520] et le nouveau règlement général sur la protection des données[521] ont harmonisés les législations touchant à la protection des données, facilitant la reconnaissance des demandes d'entraides judiciaires. De plus, le règlement CE n°460/2004 instituant l'Agence Européenne chargée de la sécurité des réseaux et de l'information[522], la directive 2002/21 du 7 mars 2002[523] et la directive 2016/680[524] ont mis en place un système d'échange des informations entre les Etats membres relatif à la criminalité informatique[525]. Mais selon certaines études, une grande partie des menaces proviennent de pays tiers[526]. Or, cette présence hors du territoire Européen entraine des difficultés d'ordre juridique.

254. La première de celles-ci, face à une intrusion informatique provenant d'un pays tiers, provient de la qualification de la compétence des juridictions Françaises pour obtenir l'identité de l'auteur de l'infraction. Selon le code de procédure pénale, la compétence territoriale est acquise si un fait constitutif de l'infraction a eu lieu sur le territoire de la République[527], ou si l'intérêt de la nation est concerné[528]. Pourtant, si les forces de l'ordre et les tribunaux sont compétents pour procéder à l'identification des adresses IP incriminées en

520 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

521 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

522 Règlement (CE) n°460/2004 du Parlement Européen et du Conseil du 10 mars 2004, *Instituant l'Agence Européenne chargée de la sécurité des réseaux et de l'information*, Journal Officiel de l'Union Européenne du 13 mars 2004. L 77.

523 Directive 2002/21/CE du Parlement Européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques, OJ L 108, 24 avril 2002, pp. 33-50.

524 Directive 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement de données à caractere personnel par les autorités compétentes à des fins de prevention et de detection des infractions pénales, d'enquetes et de poursuites en la matiere ou d'execution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la decision cadre 2008/977/JAII du Conseil, JOUE, 4 mai 2016, L 119/89.

525 Ibid, article 2.

526 v. Trend Micro, *Rapport de sécurité pour le 1er trimestre 2016*, disponible sur http://www.trendmicro.fr/newsroom/pr/le-rapport-de-securite-de-trend-micro-pour-le-premier-semestre--met-en-avant-la-recrudescence-des-ransomware-et-des-arnaques-bec-business-email-compromise/index.html (consulté le 01/09/17).

527 v. Articles 42, 382, 113-1 et 113-2 du Code de procédure pénale.

528 Articles 113-10 du Code de procédure pénale : « *la loi pénale Française s'applique aux crimes et délits qualifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés par le titre Ier du livre IV, à la falsification et à la contrefaçon du sceau de l'Etat, de pièces de monnaie, de billets de banque ou d'effets publics réprimés par les articles 442-2, 442-2, 442-5, 442-15, 443-1 et 444-1, et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires Français, commis hors du territoire de la République* ».

France, il faudra nécessaire une décision d'exéquatur, ou un mécanisme prévu par un traité, pour que l'identité de la personne détentrice de l'accès soit fournie par un opérateur étranger, qui n'agira qu'en vertu d'une décision sur son sol. Par conséquent, selon Jacques Francillon : « *la cyber délinquance et la cybercriminalité soulèvent sur le plan juridique des questions d'autant plus difficiles à résoudre qu'elles affectent une société globalisée. Cette situation rend a priori la régulation illusoire à un niveau exclusivement national, territoriale. Elle impose donc de mettre en place un cyber contrôle à l'échelle régionale, voire mondiale* »[529].

255. La solution est d'établir, au niveau international, un mécanisme automatique de reconnaissance mutuelle des décisions juridiques en matière de cybercriminalité, ainsi qu'un système d'entraide international à l'identification des auteurs d'infractions. De cette initiative, le Conseil de l'Europe fut précurseur en élaborant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[530], dont les articles 15 et 16 fondent les bases d'une procédure d'assistance en matière de traitement de données à caractère personnel. Ces principes seront repris en grande partie, puis élargis par la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001[531], à valeur internationale. Selon les articles 16 et 18, les parties signataires s'engagent à conserver les données de connexion permettant l'identification des communicants, ainsi qu'à les produire aux autorités tiers habilitées.

256. Afin d'expliquer simplement le mécanisme de fonctionnement, on peut citer Mireille Ballestrazzi, directrice centrale de la police judiciaire et présidente du comité exécutif d'Interpol qui déclarait en 2015 : « *Souvent l'initiative part d'un pays membre, qui identifie un certain nombre d'adresses IP problématiques et ouvre une enquête judiciaire. Internet étant mondial, les adresses IP concernent souvent plusieurs Etats. Interpol contacte alors le bureau central d'Interpol dans chaque pays concerné pour mettre en place une coopération internationale* »[532]. L'identification des auteurs repose sur ce système international d'entraide judiciaire.

529 Francillon Jacques, *Cybercriminalité : aspects de droit pénal international*, rapport présenté à l'association international de droit pénal, XIX congres international de droit pénal, 12 juin 2013, p. 4.

530 Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, Strasbourg, 21 janvier 1981.

531 Convention du Conseil de l'Europe sur la cybercriminalité faite à Budapest le 23 novembre 2001.

532 Ballestrazzi Mireille, propos recueillies par Sylvain Rolland, *La Cybercriminalité est la nouvelle menace du XXIeme siècle*, La tribune, 26 juillet 2015, disponible sur http://www.latribune.fr/technos-medias/internet/la-

257. Toutefois, en dehors de ces textes, on peut déplorer le manque de reconnaissance juridique des déclarations de principes issues des deux sommets mondiaux sur la société de l'information[533], ainsi que l'absence de grands pays parmi les signataires de la convention, tels que la Chine ou la Russie. Absence qui profite à un grand nombre de cybercriminels se servant de ces pays comme d'une plateforme pour lancer leurs attaques, pariant sur les difficultés administratives et juridiques qu'engendrerait une tentative des autorités d'obtenir leurs identités.

258. L'efficacité du dispositif Français de répression des atteintes aux systèmes de traitement de données n'est pas à chercher dans la législation Française mais dans les mesures juridiques internationales ayant pour but d'identifier les auteurs d'infractions quel que soit leur origine. À défaut d'un mécanisme globalisé d'échange de ces informations, le régime souffre d'un manque de portée qui est dommageable aux citoyens, principales victimes de ces actes répréhensibles. Ce manque d'efficacité est d'autant plus flagrant lorsque l'on examine les possibilités d'anonymisation des communications qui sont disponibles, et dont s'empare progressivement les cybercriminels, à l'instar des citoyens, afin d'échapper aux divers systèmes de collecte d'information, étatiques ou privés.

2 – La démocratisation des technologies d'anonymisation et de sécurisation des données

259. Il existe de nombreuses méthodes permettant d'anonymiser les moyens de communication ou de sécuriser les données. Devenu un marché à part entière, ces nouveaux outils se vantent de fournir aux citoyens des moyens de communiquer en tout sécurité. Exemple de cet écosystème, Signal[534], application développée par Open Wisper Systems, a bénéficié du soutien indirect d'Edward Snowden qui l'a utilisé lors de ses échanges avec

cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html (consulté le 01/09/17).

533 Sommet mondial sur la société de l'information, Genève, 10-12 décembre 2003 et Tunis, 16-18 décembre 2005.

534 Application Signal – Private Messenger, distribuée par Open Whisper Systems sur plateforme Android et IOS.

Glenn Grennwald[535]. Celle-ci chiffre les communications de bout en bout par l'utilisation du protocole ZRTP, qui résistait selon Der Spiegel aux attaques de la NSA en 2012[536]. Or, si cette application semble une opportunité pour les lanceurs d'alertes, une application similaire, Telegram, servait au même moment de plateforme à l'organisation Etat Islamique pour recruter et diriger des opérations terroristes[537].

260. La problématique posée par ce type de technologies est qu'elles s'opposent, de par leur conception technique, à toute forme d'interception. Par conséquent, lorsque les services régaliens souhaitent accéder de manière licite à des données, les concepteurs leurs démontrent l'impossibilité technique de satisfaire cette requête. Ce fut notamment le cas aux Etats Unis lorsque le Federal Bureau of Investigation (FBI) a souhaité accéder aux données du téléphone Apple de l'un des auteurs de l'attentat terroriste de San Bernardino en 2015. En l'espèce, le téléphone était chiffré à l'aide d'une technologie propriétaire de la marque du téléphone, qui refusait de produire un outil capable de casser ce chiffrement[538].

261. Ces exemples montrent le basculement technologique que l'innovation numérique est en train de produire. Avec les progrès récents des techniques de chiffrement et d'anonymisation des télécommunications, la difficulté des forces Etatiques dans la recherche d'informations sur les auteurs d'infractions augmente considérablement. La démocratisation de ces technologies, qu'il s'agisse de Bitcoins, de Virtual Private Network (VPN) ou d'applications spécialisées, rend d'autant plus complexe la mise en œuvre des régimes applicables aux interceptions judiciaires ou administratives. Dans ce contexte, l'équilibre entre protection du secret des communications, droit au respect de la vie privée et sauvegarde des prérogatives des services régaliens tient à la définition technique des méthodes admissibles de chiffrement.

535 v. Greenwald Glenn, *Nulle Part où se Cacher*, JC Lattès, 14 mai 2014, 280 p.

536 Applebaum Jacob, Gibson Aaron et. al., *Inside the NSA's war on internet security*, Spiegle.de, 26 decembre 2014, disponible sur http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html (consulté le 01/09/17).

537 Ouest France, *Terrorisme : la messagerie Telegram donne du fil à retordre aux policiers*, Ouest France, 16 septembre 2016, disponible sur http://www.ouest-france.fr/terrorisme/terrorisme-la-messagerie-telegram-donne-du-fil-retordre-aux-policiers-4495497 (consulté le 01/09/17).

538 Perez Evan, Hume Tim, *Apple Opposes judge's order to hack San Bernardino shooter's,* CNN, disponible sur http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html (consulté le 01/09/17).

262. Une telle définition existe déjà dans l'ordre juridique Français. Longtemps considérés comme illicites[539], ces techniques sont, selon leurs natures, classés dans la catégorie des biens « *très sensibles* », où assimilés à du matériel de guerre, par le règlement n°428/2009 du Conseil[540]. Les opérations de transferts, d'importations ou d'exportations relèvent d'un régime strict. Le décret n°2007-663 du 2 mai 2007 dresse à cette fin une liste de critères d'appréciation technique, en soumettant les outils dont le niveau de chiffrement dépasse certains seuils à un régime déclaratoire ou d'autorisation auprès du premier ministre[541]. Habilitée par le premier ministre, c'est l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui se charge d'analyser les technologies en faisant la distinction entre moyen de cryptologie et « b*iens à double usage* » selon le niveau de complexité des algorithmes et des fonctionnalités. En fonction de son évaluation, celle-ci délivrera une autorisation ou demandera au concepteur de modifier son outil. Dans l'éventualité où ces formalités ne seraient pas accomplies, le responsable encourt une contravention de 5eme classe[542].

263. Mais si les conditions d'importations sont strictes, l'utilisation n'est pas soumise à ce régime. Selon l'article 30-1 de la loi pour la confiance dans l'économique numérique, l'utilisation des moyens de cryptologie est libre[543]. De plus, il existe une exception d'utilisation personnelle, pour laquelle aucune déclaration ni autorisation n'est requise[544]. Ces applications sont donc pour la plupart, dispensées des formalités de déclaration ou d'autorisation, et leur utilisation est libre si elle n'implique pas la commission de délit[545].

---

539 Lucas Michael, *PGP et GPG : Assurer la Confidentialité de ses E-mails et Fichiers*, Eyrolles, 31 août 2006, p. 2.

540 Règlement (CE) n°428/109/CE du Conseil du 5 mars 2009 *instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage*, Journal officiel de l'Union Européenne du 29 mars 2009, OJ L 134, pp. 1-269.

541 Décret n°2007-663 du 2 mai 2007 *pris en application des articles 30,31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relative aux moyens et aux prestations de cryptologie*, JORF n°104 du 4 mai 2007, p. 7865, texte n°1.

542 Ibid. article 13.

543 Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2, article 30-1.

544 Agence Nationale de la Sécurité des Systèmes d'Informations, *Contrôle règlementaire de la cryptographie*, *Démarches à accomplir*, voir tableau de synthèse disponible sur www.ssi.gouv.fr (consulté le 01/07/17).

545 En effet, à des fins de dissuasion, la loi pour la confiance dans l'économie numérique augmente drastiquement les peines encourues en cas d'utilisation des technologies de cryptologie pour préparer ou commettre un crime ou un délit, ou pour en faciliter la préparation ou la commission d'un crime ou d'un délit en créant l'article 132-79 du code pénal. v. Article 132-79 du code pénal, créé par Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2, article 37.

264. Face à cette exception au régime et à cette limite technologique, les services régaliens peuvent tout de même s'appuyer sur différentes dispositions en fonction de l'état d'avancement de l'enquête. Dans un premier temps, il s'agira d'obtenir les données brutes chiffrées, puis dans un second, d'y accéder en clair. À cette fin, les articles 60-1 et 60-2 du code de procédure pénale, déjà évoqués au point 221 de cet ouvrage, indiquent que le procureur de la République ou l'officier de police judiciaire peut requérir de toute entité publique ou privée les informations qu'elle détient sur une personne intéressant l'enquête, notamment sous forme numérique. Ces dispositions permettent, sous le régime des interceptions administratives ou judiciaires, d'obtenir les données brutes et chiffrées qui sont stockés par les services de télécommunications ou par les fournisseurs de réseaux.

265. Une fois en possession des services, les données doivent être déchiffrées. Pour faciliter cette tâche, le législateur a récemment modifié l'article 434-15-2 du code pénal avec la loi du 3 juin 2016[546], qui « *puni de trois ans d'emprisonnement et de 279 000 euro d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités* ». En outre : « *si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 euro d'amende* ». Dans le cas où la personne ou l'entité refuserait de fournir ces renseignements, le procureur de la République, la juridiction d'instruction ou l'officier de police judiciaire pourront faire application de l'article 230-1 du code de procédure pénal, en désignant toute personne physique ou morale qualifiée pour effectuer des opérations de déchiffrement. Si la peine encourue est supérieure ou égale à deux ans, les moyens de l'Etats soumis au secret de la défense nationale peuvent être mis à disposition.

266. Cependant, au-delà de ces dispositions juridiques, certaines méthodes de chiffrement sont aujourd'hui réputées inviolables, tel que la méthode RSA 1024, utilisée pour une grande partie des échanges sécurisés sur internet[547]. Sur la base de cette constatation, le ministre de

546 Loi n°2016-737 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, texte n°1.

547 v. Mutyaba Robert, *Improving the RSA Cryptographic Algorithm*, Lambert Academic Publishing, 2010, 84 p.

l'intérieur, Bernard Cazeneuve, a récemment déclaré travailler avec son homologue Allemand sur la possibilité de présenter un texte au niveau Européen, tendant à limiter juridiquement la complexité des algorithmes, en permettant aux autorités de les « *casser* » en cas de nécessité[548]. Face à cette possibilité, une grande partie du Conseil National du Numérique et Isabelle Falque-Pierrotin, présidente de la CNIL se sont exprimés dans une tribune commune en rappelant l'importance de ces technologies pour le public et l'industrie : « *c'est grâce au chiffrement que nous pouvons effectuer un virement bancaire en toute sécurité. C'est grâce au chiffrement que nous pouvons stocker nos données de santé dans un dossier médical partagé (DMP). C'est également grâce à cet outil que les investigations sur les Panama Papers ont été possibles, le chiffrement permettant de garantir le secret des sources. Pour les entreprises, le chiffrement est aujourd'hui le meilleur rempart contre l'espionnage économique qui a fait perdre plus de 40 milliards d'euros aux entreprises Françaises en 2013* »[549]. De fait, en limitant le recours aux technologies de chiffrement difficilement contournables, la loi aurait pour effet de faciliter également la commission des infractions utilisant cette vulnérabilité.

Conclusion

267. Devant l'innovation numérique, le droit fait face à une double difficulté. D'une part, sa structure territorialisée reste dépendante de la volonté coordonnée des Etats de fixer, au niveau international, des normes communes ayant pour but de sanctionner les auteurs d'infractions numériques. D'autre part, en fournissant des moyens de cryptographie de plus en plus techniques, l'innovation entre en conflit direct avec les prérogatives régaliennes relatives aux acquisitions de données.

268. Si la difficulté liée à l'ubiquité d'internet peut être surmontée juridiquement et relève d'une volonté essentiellement politique, la limitation de l'utilisation des technologies de chiffrement s'oppose, par essence, aux objectifs de sécurisation des échanges numériques. En effet, en constatant l'inefficacité des mesures de répression de la cybercriminalité, le droit au

548 Le Monde.fr, *Bernard Cazeneuve veut « une initiative Européenne » contre le chiffrement*, Le Monde, 12 août 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/08/12/bernard-cazeneuve-veut-une-initiative-europeenne-contre-le-chiffrement_4981741_4408996.html (consulté le 01/09/17).

549 Conseil National du Numérique, *Tribune : chiffrement et lutte contre le terrorisme, attention à ne pas se tromper de cible,* disponible sur https://cnnumerique.fr/tribune-chiffrement/ (consulté le 01/09/17).

respect de la vie privée dépend essentiellement de la capacité des citoyens et des entités privées et publiques à sécuriser l'accès aux données.

269. Dans cet environnement technologique ou la sécurité des informations et les possibilités d'interceptions administratives et judiciaires doivent se conjuguer, un élément de réponse pourrait se trouver dans le développement de standard technique de protection, à travers la mise en place généralisée de la Privacy By Design.

Chapitre 2

Une réinterprétation technique de la protection offerte par le régime

*

270. Il existe une difficulté inhérente au droit lorsqu'il s'agit d'appliquer des définitions juridiques générales dans un environnement technique précis[550]. Dans le cadre du régime de protection des données à caractère personnel par exemple, les notions de traitements de données, d'accès, de stockage ou de transfert peuvent être interprétées de différentes manières par un responsable de traitement, a fortiori quand la justice Française hésite elle-même, à tort[551], sur la qualification de l'adresse IP comme données à caractère personnel. Par conséquent, le respect des mesures de protection relève de deux facteurs : une traduction technique précise des mesures juridiques en amont et un contrôle efficace en aval par les autorités indépendantes et les personnes concernées.

550 A titre d'exemple, on peut citer le projet ASPHALES financé dans le cadre de l'Action Concertée Incitative (ACI) 2004, dont l'IREENAT de l'université Lille 2 fut partenaire, ayant pour objectif d'étudier les problématiques posées par les interactions entre le vocabulaire juridique et les réponses techniques.

551 Même si la CNIL a rappelé dans sa communication du 2 août 2007 qu'une adresse IP était une donnée à caractère personnel, en réponse à la décision du 15 mai 2007 de la Cour d'Appel de Paris qui en donnait une interprétation différente, la chambre criminelle de la Cour de Cassation refusait le 13 janvier 2009 d'appliquer le régime protecteur, de même que la Cour d'Appel de Rennes le 28 avril 2015. v. Cass. Soc., 13 janvier 2009, n°07-43282, Bull. Soc. 2009, V, n°3.

271. Cependant la Commission Européenne semble avoir une approche différente : « *bien qu'à strictement parler, ce soient les responsables du traitement qui sont juridiquement responsables de l'observation des règles de protection des données, les personnes qui conçoivent les caractéristiques techniques, et celles qui effectivement produisent ou mettent en œuvre des applications ou des systèmes d'exploitation, portent également une part de la responsabilité à l'égard de la protection des données sous l'angle des questions de société et d'éthique* »[552]. Dans une telle perspective, la responsabilité du respect du régime de protection se déplace sur le terrain de la conception technique.

272. L'avantage d'une telle prise en compte est que les mesures protectrices sont considérées comme faisant partie intégrante du processus de conception d'un outil technologique, limitant de facto les possibilités d'infractions au régime lors de l'utilisation finale. De même, celles-ci peuvent intégrer les besoins nécessaires à la mise en œuvre des régimes d'interceptions administratives et judiciaires, garantissant l'application du droit dans le domaine numérique. Selon la Commission : « *le recours aux technologies renforçant la protection de la vie privée permet de concevoir des systèmes et des services d'information et de communication qui réduisent la collecte et l'utilisation de données à caractère personnel et à faciliter le respect des règles de protection des données. Grace à l'utilisation des technologies renforçant la protection de la vie privée, les infractions à certaines règles de protection des données devraient être plus difficiles à commettre et/ou plus faciles à détecter* » [553]. Un système conçu selon cette acception intègre ce que la Commission nomme une « *technologie renforçant la protection de la vie privée* », autrement appelé PET pour Privacy Enhancing Technology. Il peut s'agir de différentes couches logicielles ayant trait chacune à l'un des aspects du traitement, comme une anonymisation automatique des données, un procédé de chiffrement généralisé limitant les possibilités d'extraction frauduleuse, voire de modification d'interface pour l'utilisateur, avec la mise en place d'une plateforme de préférences relatives à la protection de la vie privée.

552 Commission Européenne, *Technologies renforçant la protection de la vie privée*, Mémo 07/159, Bruxelles, 2 mai 2007.
553 Ibid.

273. Imaginé dès 1995, l'intégration de ces moyens techniques est en passe de devenir obligatoire à l'horizon 2018, avec l'application de l'article 25 du règlement général sur la protection des données[554]. Ce nouveau régime confirme l'intégration juridique de la Privacy By Design au processus d'innovation (section 1), sans que soient adressés les dangers que soulève la réinterprétation technique des protections juridiques (section 2).

Section 1

L'intégration juridique de la Privacy by Design au processus d'innovation

274. C'est en 1995 que le concept apparait pour la première fois, dans un rapport visant à démontrer l'importance d'une prise en compte technique de la protection de la vie privée dans les technologies[555]. Cette approche suggérait la possibilité de limiter au niveau technique la quantité de données à caractère personnel à ce qui était strictement nécessaire aux fonctionnalités d'un produit ou d'un service. Le terme utilisé alors était celui de PET, et fut progressivement enrichi par la doctrine pour englober l'ensemble des fonctionnalités techniques ayant pour objet de limiter les possibilités d'atteinte au droit au respect de la vie privée, telles que les techniques d'anonymisations[556] ou les interfaces utilisateurs permettant de choisir l'exposition de ses données[557].

554 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

555 v. Borking John, *Privacy Enhancing Technologies*, Based on a Joint Study in Netherlands and Ontario, 1995 ; Borking John, Van Eck B.M.A, Spiepel P., *Intelligent Software Agents and Privacy*, Registratiekamer, The Hague, janvier 1999, 73 p.; Hustinx Peter, Communication, *Respect de la vie privée dès la conception (Privacy by Design): le séminaire définitif*, Madrid, 2 nov. 2009, disponible sur http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf (consulté le 01/09/17).

556 v. Goldberg Ian, Wagner David, Brewer Eric, *Privacy-Enhancing technologies for the Internet*, Proceedings IEEE COMPCON 97, Digest of Papers, San Jose, CA, USA, 1997, pp. 103-109.

557 v. Wang Yang, Kobsa Alfred, *Privacy-Enhancing Technologies*, Handbook of research on social and organizational liabilities in information security, IGI Global, 2009, pp. 203-227.

275. L'idée générale fut reprise en grande partie par Ann Cavoukian qui proposa le concept devenu aujourd'hui la norme[558], de Privacy By Design à la fin des années 90. Celui-ci repose sur sept principes. *Proactivité,* consistant à prévenir en amont les risques pensant sur les données. *Une protection par défaut* des données, en minimisant le risque d'exposition involontaire. *Une protection intégrée* au design du produit lors de sa conception, afin d'éviter les difficultés qu'entraineraient une refonte de son architecture. *Une protection à somme positive,* pour s'intégrer au mieux dans un environnement complexe mêlant risques techniques et nécessités économiques. *Une protection de bout en bout*, jusqu'à la destruction des données. *Une protection transparente*, afin que l'utilisateur puisse avoir une plus grande confiance dans le produit. Et enfin, *une protection centrée sur l'individu,* où celui-ci sera capable de choisir le niveau d'exposition de ses données[559].

276. Bénéficiant d'une grande publicité, la Privacy By Design s'est progressivement diffusée pour devenir un outil de conception produit recommandé par les autorités indépendantes. Le G29 prône ainsi son utilisation pour les nouveaux produits issus de l'internet des objets[560]. De plus, celle-ci est plébiscitée par les industriels. Selon David Hoffman, directeur de la politique de sécurité chez Intel : « *Intel voit la Privacy By Design comme un composant nécessaire des mécanismes d'audit que nous intégrons à nos produit et au service des processus de développements. Nous applaudissons le fait que le rapport reconnaisse que le cadre de la protection de la vie privée soit nécessairement intégré comme un principe dans les produits et les services* »[561]. Pour les représentants de l'économie numérique, l'intérêt est double. Tout d'abord, la PbD permet d'assurer la sécurité juridique des investissements en limitant le risque d'exposition aux sanctions en cas d'intrusion

558 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

559 Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, Ontario, Canada, December 2012.

560 Groupe de Travail « Article 29 » sur la protection des données*, Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, adopté le 16 septembre 2014, 1471/14/FR, WP 223.

561 Traduction par l'auteur de : « *Intel views Privacy By Design as a necessary component of our accountability mechanisms that we implement in our product and service development processes. We applaud the report's recognition that a privacy framework should specifically require that organizations ensure that privacy is included as a principle in product and service development processes* ». Hoffman A. David, *FTC Staff Preliminary Report on Protecting Consumer Privacy*, File n°P095416, January 26 2011, disponible sur https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00246-57451.pdf (consulté le 01/09/17).

frauduleuse ou de traitement illicite des données des utilisateurs. Ensuite, elle constitue un véritable objet marketing, tendant à démontrer aux utilisateurs potentiels qu'un produit ayant intégré ces caractéristiques leur est favorable. Selon Ann Cavoukian: « *le respect de la vie privée a toujours été une norme sociale, mais depuis quelques années, il a évolué. Il ne s'agit plus désormais de respecter simplement la loi, mais également de se démarquer sur le marché, de mériter la confiance des consommateurs et de favoriser le libre choix dans notre société de l'information* »[562].

277. Pourtant, la PbD reste un concept difficile à cerner. Lorsque l'on examine la définition de ses critères, aucune précision n'intervient quant aux aspects techniques qu'ils impliquent. Ceux-ci ne proposent pas de standard technique de protection, alors même qu'une norme ISO existe déjà en ce qui concerne les systèmes de gestion de la sécurité de l'information[563]. Dès lors, il sera nécessaire pour chaque entité d'évaluer elle-même le niveau de sécurité optimal des informations qu'elle détient, ainsi que la manière dont elle propose aux utilisateurs de gérer leurs données. Cet état de fait peut conduire à une hétérogénéité des protections, voire à une réduction de celles-ci comme semble l'annoncer Jean-Jacques Lavenue lorsqu'il compare la Privacy By Design à un cheval de Troie[564], alors même que le concept sera un standard juridique à l'horizon 2018.

278. Pour comprendre les conséquences de l'entrée de ce concept dans l'ordre juridique Européen avec le règlement général sur la protection des données, il convient de déterminer de quelle manière une entité peut intégrer techniquement la Privacy By Design au processus d'innovation (1), puis d'examiner un exemple concret d'application, avec celui de l'intégration de la technologie dite « *de base de données à lien faible* » dans la base de données des passeports Français (2).

562 Cavoukian Ann, déclaration disponible sur http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles-f.pdf, (consulté le 01/02/17).

563 v. la famille de normes ISO/IEC 27000 pour les systèmes de gestion de sécurité de l'information, dont la norme ISO/IEC 27001 est utilisée dans le cadre des règlementations relatives aux données de santé.

564 v. Lavenue Jean-Jacques, *La Privacy By Design : Panacée ou cheval de Troie ?,* Revue de la Recherche Juridique, Droit Prospectif, 2013-1, pp. 59-73.

1 – L'intégration technique de la Privacy By Design au processus d'innovation

279. Le premier principe énoncé par Ann Cavoukian est celui de la nécessaire proactivité de la Privacy By Design. Pour cela, il faut que les mesures d'ordre technique ayant trait à la sécurité des données soient intégrées dès la phase de conception du produit, sur la base d'un processus d'évaluation du risque[565]. C'est en grande partie ce que reprend la formulation de l'article 25 du règlement général de protection des données. Selon le premier alinéa : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* »[566]. Dès lors, tout processus de Privacy By Design repose sur l'exactitude de l'évaluation du risque.

280. C'est ce que l'on nomme un Privacy Impact Assessment, ou PIA, pour étude d'impact sur la vie privée. Celui-ci repose sur deux piliers : les principes et les droits fondamentaux, qui sont fixés par la loi, et la gestion des risques sur la vie privée des personnes concernées[567]. Selon l'article 35 du RGPD, il doit comprendre au minimum « *une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ; une évaluation de la nécessité de la proportionnalité des opérations de traitement au regard des finalités ; une évaluation des risques pour les droits et les libertés des personnes concernées ; les mesure*

565 Ibid.

566 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

567 Commission Nationale de l'Informatique et des Libertés, *PIA : La méthode*, CNIL, Edition juin 2015, p. 4.

envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées »[568]. De plus, lorsqu'il se produit une modification du risque en cours de traitement, le responsable est chargé d'évaluer une nouvelle fois, si nécessaire, l'ensemble de la procédure.

281. Afin d'aider les responsables de traitement à mener cette étude, la CNIL a publié en juin 2015 une méthodologie de mise en œuvre du PIA[569]. Celle-ci permet d'identifier les mesures organisationnelles de sécurité physique et de sécurité logique qui doivent être mise en œuvre, tout en rappelant l'importance des mesures transversales de gouvernance de la protection de la vie privée. Selon cette méthode, quatre étapes successives d'analyses doivent être développées. La première consiste en une analyse du contexte lié au traitement et aux données recueillies. La seconde sert à identifier les mesures existantes (légales ou techniques) ayant pour but de traiter les risques pesant sur la vie privée des personnes concernées. La troisième phase est une évaluation des risques potentiels pesant sur la sécurité du traitement et des informations. Enfin, la quatrième étape consiste en la validation des contres mesures à déployer en fonction des éléments particuliers du traitement.

282. La mise en œuvre d'un PIA reste une difficulté puisqu'il nécessite la mise en commun de compétences juridiques, concernant les règlementations applicables à la sécurité des données, et techniques vis-à-vis de leurs intégrations au produit. Pour cela, et à cause de l'aspect hautement confidentiel d'un tel document, nous ne pouvons reproduire un exemple concret de PIA dans cet ouvrage. Cependant, à titre d'exemple, l'annexe de la communication du G29 présente un modèle de Privacy Impact Assessment pour les technologies de Radio Frequency Identification (RFID)[570] est disponible en annexe.

568 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 35.

569 Commission Nationale de l'Informatique et des Libertés, *PIA : La méthode*, CNIL, Edition juin 2015, p. 4.

570 Groupe de travail « Article 29 » sur la protection des données, *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12 January 2011, WP 180.

283. Néanmoins, afin d'aborder la philosophie qui accompagne un PIA, nous pouvons prendre l'exemple, novateur pour l'époque, de l'idée d'intégrer une technologie de base de données à lien faible lors de l'examen de la loi relative à la protection de l'identité du 27 mars 2012, qui a entrainé une modification des dispositifs techniques liés au traitement des données des passeports biométriques[571]. En effet, cet exemple est emblématique de la problématique de l'appréciation du risque technologique et de la réponse technique dont peut dépendre le respect du droit au respect de la vie privée, et cela, avant même le développement des méthodologies de mise en œuvre des PIA.

2 – L'exemple de l'intégration potentielle d'une base de données à lien faible pour les passeports biométriques

284. Un PIA est l'élément central de la PbD. Il s'agit d'examiner, à chaque niveau, l'ensemble des menaces pesant sur le traitement, afin de mettre en place au niveau technique les pratiques ou technologies susceptibles de lui assurer une sécurité maximale. Celui-ci doit intervenir au plus tôt dans la phase de développement. En effet, une modification technique est d'autant plus complexe qu'elle est envisagée tard dans le processus d'innovation, plus encore lorsqu'il s'agit d'adapter un produit ou une base de données déjà existante. On peut trouver une illustration de cette problématique dans le débat législatif qui a entouré la création de la loi relative à la protection de l'identité du 27 mars 2012[572].

285. Le 27 juillet 2010, les sénateurs Jean-René Lecerf et Michel Houel déposent une proposition de loi pour « *garantir une fiabilité maximale aux passeports et aux cartes nationales d'identités, afin de lutter contre les délits liés à l'usurpation d'identité et à la fraude documentaire* » [573]. Cette proposition fait suite à un constat établi par l'un des auteurs de la proposition dès 2005[574], qui relève que lorsqu'il s'agit d'identifier une personne,

571 Loi n°2012-410 du 27 mars 2012, *relative à la protection de l'identité*, JORF n°0075 du 28 mars 2012, p. 5604, texte n°2.
572 Loi n°2012-410 du 27 mars 2012, *relative à la protection de l'identité*, JORF n°0075 du 28 mars 2012, p. 5604, texte n°2.
573 Proposition de loi relative à la protection de l'identité, présentée par MM. Jean-René Lecerf et Michel Houel, Texte n°682, enregistré à la présidence du Sénat le 27 juillet 2010.
574 Lecerf Jean-René, *Rapport d'information n°439 fait au nom de la commission des lois et de la mission*

l'efficacité du contrôle dépend de la capacité du dispositif à s'appuyer sur des éléments infalsifiables. Selon lui, « *les modes traditionnels de preuve de l'identité [étaient] affaiblis* » [575]. De même, « *aucun organisme ou ministère n'a réalisé une évaluation globale de la fraude à l'identité en France* » alors même que « *les principaux points faibles de la chaine de l'identité se situent au niveau de l'état civil et du vol de documents vierges* » [576]. Dans ce contexte, un renforcement de l'informatisation des titres de voyages et d'identité est proposé, avec l'intégration systématique d'une puce qui contiendra les informations biométriques de l'individu. De plus, le rapport prône une centralisation des bases de données relatives à l'identité des citoyens afin de détecter plus facilement les tentatives de fraudes et les doublons.

286. La proposition de loi reprendra logiquement les propositions avancées dans le rapport sénatorial[577]. Mais si l'informatisation des titres d'identité ne semble pas créer de polémique[578], la centralisation des bases de données pose des problématiques touchant directement à notre étude. De fait, la centralisation d'une base de données, à fortiori de la sensibilité des données identifiantes et biométriques des citoyens Français, engendre un niveau de risque conséquent vis-à-vis du droit au respect de la vie privée. En cas d'intrusion, le dommage serait extrêmement important en termes de quantité de données, mais également au regard de la qualité des données qui peuvent ensuite servir à de multiples usurpations d'identités. Dans le cadre d'un PIA, cette spécificité de la base de données entrainerait logiquement une réflexion sur la constitution technique de celle-ci et c'est justement sur ces caractéristiques techniques, aux conséquences juridiques palpables, que le débat s'est cristallisé. Selon le rapport précité, il existe trois méthodes différentes d'organisations techniques d'une telle base de données[579].

---

d'information de la commission des lois, Séant, Annexe au procès-verbal de la séance du 29 juin 2005, p. 51.

575 Ibid, p. 51.

576 Ibid, p. 7.

577 Proposition de loi relative à la protection de l'identité, présentée par MM. Jean-René Lecerf et Michel Houel, Texte n°682, enregistré à la présidence du Sénat le 27 juillet 2010, article 5.

578 Notamment dans un contexte sécuritaire post-11 septembre 2001, qui a vu l'Europe se doter de nouvelles normes biométriques en matière de passeports et de documents de voyage, avec le Règlement (CE) n°2252/2004 du Conseil, du 13 décembre 2004 *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres*, Journal officiel de l'Union Européenne du 29 décembre 2004, L 385/1.

579 Lecerf Jean-René, *Rapport d'information, fait au nom de la commission des lois et de la mission d'information de la commission des lois*, n°439, 29 juin 2005, p65.

287. La première est une base de données décentralisée dans laquelle les données biométriques ne figurent que sur la puce. Avec un tel système, il suffit de vérifier la corrélation du gabarit d'empreinte enregistrée lors de la création du titre avec l'empreinte que présente la personne sur un capteur. Si elles correspondent, la personne est bien la titulaire du titre. Une telle solution est satisfaisante pour la protection de la vie privée en diminuant drastiquement les possibilités d'atteinte aux informations, mais dans ce cas, le contrôle de l'unicité est impossible. De même, la falsification initiale lors de la création d'un titre ne peut pas être détectée au regard de l'impossibilité de comparer l'empreinte de la personne aux données déjà liées à d'autres identités. Enfin, en cas de tentative de fraude, il n'est pas possible de consulter l'ensemble du fichier pour retrouver l'identité d'un individu à partir de ses empreintes.

288. Une seconde méthode consiste en une centralisation des bases de données. Avec ce système, la détection des doublons est possible ainsi que la recherche de l'identité du fraudeur à partir de ses empreintes. La procédure de remplacement d'un titre en cas de perte est grandement facilitée, puisqu'elle ne nécessite pas un second enrôlement[580] dans la base de données. Par conséquent, des révocations peuvent être réalisées à distance. Toutefois, ce système présente le désavantage de réunir en un lieu unique un grand nombre d'informations, qui sont à la disponibilité de nombreux services régaliens. De par ses possibilités d'accès, le risque d'un détournement, volontaire ou non, est considérable.

289. Une troisième méthode existe, fondée sur une base de données à lien faible. Selon le rapport sénatorial de M. Philippe Goujon en date du 29 juin 2011 : « *Dans ce système, plusieurs dizaines ou centaines de milliers d'empreintes sont associées à plusieurs dizaines ou centaines de milliers d'identités sans qu'un lien soit établi entre une de ces empreintes et l'une de ces identités. Nul ne peut en conséquence être identifié à partir de ses seules empreintes digitales, ce qui interdit l'utilisation du fichier à des fins de recherche criminelle, en l'absence d'autres indices impliquant l'intéressé* » [581]. Toujours selon le rapport : «*cette technologie permet de s'assurer de l'identité d'un individu, par la comparaison entre*

580 Enrôlement : procédé technique de captation des informations biométriques d'un individu.

581 Goujon Philippe, *Rapport n°3599 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la proposition de loi n°3471 adoptée par le Sénat, relative à la protection de l'identité*, enregistré à la présidence de l'Assemblée Nationale le 29 juin 2011, p. 12.

l'identité qu'il allègue et les données associées à cette identité. Les chances qu'un individu qui souhaiterait usurper l'identité d'une autre personne possède des empreintes biométriques correspondant à celles susceptibles d'être associées à l'identité en cause sont en effet très faibles et inférieures à 1 %. Il a [le rapporteur] *estimé, en conséquence, que l'usurpation d'identité devenait impossible, car trop risquée* » [582]. Ce système présente une difficulté en cas d'identification, car seule la phase d'enrôlement lie l'identité et la donnée biométrique. Cette méthode ne permet donc pas de rechercher les auteurs d'infractions à partir de leurs empreintes.

290. Dans le cadre d'un PIA, le système de base de données à lien faible devrait être retenu, d'abord à cause de la finalité du traitement, ayant pour but d'authentifier les personnes à partir de leurs titres d'identités, mais aussi compte tenu des risques pesant sur la centralisation des données. Ce fut d'ailleurs l'avis de la CNIL. Dans une note d'observation produite après la première lecture du texte, celle-ci va considérer que : « *la spécificité des données biométriques a pour conséquence d'accroitre le niveau d'exigence quant à leur utilisation. En particulier, deux principes fondateurs du droit à la protection des données à caractère personnel doivent être impérativement respectés : le principe de finalité […] et […] le principe de proportionnalité* » [583]. Dès lors, son argumentaire va peser en faveur d'une base de données à lien faible puisque celle-ci assure « *l'absence de lien univoque entre les données biométriques enregistrées dans le traitement central et les données d'état civil des personnes auxquelles ces données correspondent* »[584]. Mais si sa décision s'appuie sur une évaluation de la proportionnalité de la mesure vis-à-vis de son objectif, on peut imager que c'est bien le niveau de risque induit par le traitement qui reste le point d'achoppement, ainsi que le choix de la technologie qui sécurisera son utilisation.

291. Cette affirmation, similaire à une approche PbD, sera d'ailleurs exprimée oralement lors de l'audition de la présidente de la CNIL, Mme Falque-Pierrotin, qui déclare : « *les restrictions juridiques seront toujours moins efficaces que les restrictions techniques qui rendent impossibles l'utilisation de la base [à des fins détournées]* » [585]. Par conséquent,

582 Ibid, p. 12.
583 Commission Nationale de l'Informatique et des Libertés, Note d'observation concernant la proposition de loi relative à la protection de l'identité, Examinée en séance plénière le 25 octobre 2011, p. 3.
584 Ibid, p. 7.
585 Falque-Pierrotin Isabelle, *Déclaration publique en présence de la Commission des lois*, 14 décembre 2011.

lorsque le législateur opta définitivement le 6 mars 2012 en faveur d'une base de données à lien fort[586], le Conseil Constitutionnel fut saisi. Selon sa décision du 22 mars 2012 : « *les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins que la vérification de l'identité d'une personne* » [587]. En conséquence, celui-ci invalida les articles relatifs à la base de données centralisée, et la loi remaniée du 27 mars 2012 restera silencieuse sur la technologie choisie[588].

292. Ainsi donc, au-delà de l'argumentaire juridique orienté sur la proportionnalité de la mesure, c'est avant tout une approche de PbD que la CNIL et le Conseil Constitutionnel ont mené conjointement. En faisant une analyse des risques pesant sur le traitement, ils ont réalisés avant l'heure un PIA, et se sont prononcés en faveur d'une base de données à lien faible, à la fois plus respectueuse des droits des citoyens, mais aussi plus sure vis-à-vis des extractions illicite. Dès 2018, une approche similaire devra être mise en œuvre dans l'innovation numérique, avec la possibilité de faire basculer l'approche juridique dans une réinterprétation technique qui peut le dépasser.

586 Texte adopté n°883, Petite loi, Session ordinaire de 2011-2012, 6 mars 2012, sur la proposition de loi relative à la protection de l'identité.

587 Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, Rec. p. 158, Journal officiel du 28 mars 2012, p. 5607.

588 Loi n°2012-410 du 27 mars 2012, *relative à la protection de l'identité*, JORF n°0075 du 28 mars 2012, p. 5604, texte n°2.

Section 2

Les dangers d'une réinterprétation technique des mesures de protection

293. La PbD constitue un outil qui, comme nous l'avons observé, peut contribuer à assurer au niveau technique le droit au respect de la vie privée. Dans notre exemple sur la loi de protection de l'identité[589], il est possible d'affirmer que le recours à une base de données à lien faible pour les titres d'identités aurait eu l'avantage d'assurer à la fois la sécurité juridique et la sécurité technique du traitement. En cela, la PbD est susceptible, comme sa principale défenderesse Ann Cavoukian l'annonce, de définir des standards de protection efficace à tous les niveaux dans l'industrie et sur chaque continent. Pourtant, si l'on se base sur ces recommandations générales, un problème intervient lorsqu'il s'agit de les appliquer à un domaine particulier. Selon Anne Cavoukian: « *Le challenge est qu'il n'existe pas de taille unique ni de réponse spécifique au niveau du développement pour la protection de la vie privée. En réalité, puisque le succès de l'implémentation de la Privacy By Design réside dans les recommandations spécifiques des industriels et des développeurs d'applications, il semble improbable qu'un socle unique soit développé dans un future proche* »[590]. C'est sous cette acception que la PbD est porteuse d'une double difficulté.

294. La première relève de l'appréciation laissée aux responsables de traitement dans la qualification des risques pesant sur leurs bases de données et dans les mesures techniques à adopter. En l'absence d'uniformisation ou de normes fixées par une autorité normative, une différence d'appréciation peux exister entre une autorité indépendante et un responsable de traitement lorsqu'il s'agit de choisir les protections à mettre en place autour d'un fichier de

589 Loi n°2012-410 du 27 mars 2012, *relative à la protection de l'identité*, JORF n°0075 du 28 mars 2012, p. 5604, texte n°2.

590 Traduction par l'auteur de: « *The challenge is that there is no « one-size-fits-all » response to specific « developer-level » privacy requirements. In fact, since the successful implementation of Privacy By Design rests on the specific privacy requirements provided by business and application owners to developers, it seems improbable that a comprehensive canon of privacy requirements will be developed in the near future* ». Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, December 2012, p. 2.

données particulier. Or, une mauvaise appréciation peut constituer un manquement grave. D'abord au regard de l'impact potentiel sur la vie privée des personnes concernées, mais aussi de par l'augmentation drastique du montant des sanctions qui peuvent atteindre les entreprises, au risque de déstabiliser l'innovation.

295. La seconde est d'ordre juridique, à travers le risque d'une dépossession normative du pouvoir législatif au profit d'une normalisation technique, dont les principaux acteurs restent les GAFA. Toujours selon Ann Cavoukian : « *Alors que l'intégration d'une protection efficace de la vie privée à l'intérieur des applications deviendra commune, j'espère qu'un mouvement d'uniformisation des codes sera développé, d'autant que les développeurs partagent leurs codes pour les fonctions les plus couramment utilisées* »[591]. Cette uniformisation au niveau fonctionnel passe nécessairement par une uniformisation des pratiques des grands acteurs internet. À titre d'exemple, on peut observer le développement du standard HTML5. Prôné par Google, la technologie concurrence la technologie propriétaire Flash d'Adobe. Par défaut, le géant Californien a configuré son navigateur maison, Chrome, afin que celui-ci désactive la technologie de son concurrent[592]. De son coté, Apple a clairement opté pour la même technologie, et lui donne la priorité sur l'ensemble de ses services[593]. En conséquence, depuis le 1 novembre 2016, ce code est recommandé comme standard par le World Wide Web Consortium (W3C)[594]. Si l'on ne peut prendre position sur le débat des avantages techniques de l'une ou de l'autre des solutions, on peut supposer que la puissance des grands acteurs informatique a joué un grand rôle dans la normalisation d'une technologie. Dans le cadre de la PbD, il est nécessaire de prendre en compte cette position dominante des principaux acteurs dépendants de la possibilité de valoriser les données à caractère personnel sur les aspects normatifs des mécanismes de protection.

591 Traduction par l'auteur de: « *Certainly, as implementation of strong privacy protections within applications becomes more common, I expect that a movement toward shared code libraries will develop, much as developers share code for other commonly required functions* ». Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, December 2012, p. 2.

592 Ribeiro John, *Google Part en Guerre Contre Flash avec HTML5*, Le Monde, disponible sur http://www.lemondeinformatique.fr/actualites/lire-google-part-en-guerre-contre-flash-avec-html5-64824.html (consulté le 01/04/17).

593 Jobs Steve, *Thoughts on Flash*, April 2010, Apple.com, disponible sur https://www.apple.com/hotnews/thoughts-on-flash/ (consulté le 01/09/17).

594 W3C, W3C Recommandation, HTML 5.1, 1 november 2016, disponible sur https://www.w3.org/TR/2016/REC-html51-20161101/ (consulté le 01/09/17).

296. Dès lors, il convient d'exposer dans un premier temps l'exemple d'une différence d'appréciation dans la mise en œuvre des standards de protection avec l'exemple de la protection des répliques biométriques dans le cadre d'un projet innovant (1), puis d'analyser le risque de dépossession normatif (2) qu'engendre la PbD.

1 – Les conséquences d'une différence d'appréciation des standards de protection

297. Pour montrer les difficultés que soulève l'interprétation de la PbD, nous prendrons l'exemple d'un projet innovant, tendant à développer des contre-mesures aux différentes attaques physiques que peuvent subir les dispositifs biométriques[595]. Dans le cadre de ce projet, les ingénieurs travaillent à élaborer des faux biométriques, en se basant sur une identité réelle, afin de vérifier la solidité des algorithmes d'authentifications biométriques. Ces leurres sont des photographies, des vidéos, ou même des répliques d'iris ou d'empreintes digitales, qui seront apposées sur les capteurs afin de vérifier si le système détecte et rejette ces tentatives d'authentifications frauduleuses. L'objectif juridique dans l'accompagnement d'une telle recherche est d'obtenir une sécurité juridique optimale, afin de garantir la pérennité des investissements, ce travail s'effectuant sur une longue période. Cela implique notamment de s'assurer du respect du cadre protecteur des données à caractère personnel dès la première collecte de données jusqu'à leur destruction. Or, cette analyse met en lumière une double problématique.

298. Tout d'abord, comme dans de nombreux cas portant sur l'analyse de nouvelles données[596], il n'existe pas de position doctrinale sur la qualification juridique des répliques biométriques. Cela constitue un premier biais dans l'approche PbD. En faisant reposer la mise en place de la PbD sur la qualification d'une donnée numérique en données à caractère personnel, un responsable de traitement peut s'exonérer de la mise en place des protections suffisantes dans le cas d'une absence de reconnaissance expresse de la catégorie de données

595 Projet ANR BIOFENCE, ANR-13-INSE-0004.

596 On peut penser à la qualification de la collecte de données de connexion des imprimantes sur un réseau, ou pour certains objets technologiques comme les adresse IP des détecteurs de présences ou des caméras numériques.

qu'il traite en tant que données à caractère personnel. Dans le cadre de la procédure de la CNIL à l'encontre de Google relative au service Street View, la société Américaine a soutenu que les données SSID et MAC n'étaient pas des données à caractère personnel, faute d'une reconnaissance expresse de celles-ci. Selon celle-ci: « *Une adresse MAC est une simple identification matérielle assignée par le constructeur. Les SSIDs sont souvent le nom du routeur ou du fournisseur d'accès auquel l'on ajoute des nombres et des lettres, bien que certaines personnes les personnalisent. Cependant, nous ne collectons aucune information à propos du propriétaire et nous ne pouvons identifier une personne à partir des données géographiques que Google collecte grâce à ses véhicules* »[597].

299. Toutefois, la Commission relève que « *les identifiant SSID permettent d'identifier les réseaux Wi-Fi se trouvant à portée et de s'y connecter et que ces identifiants comportent fréquemment le nom et/ou le prénom des titulaires du réseau ; de tels éléments permettent alors manifestement d'identifier une personne physique. Ces données doivent alors être considérées comme constituant des données à caractère personnel* »[598]. De même, « *une adresse MAC, qui n'identifie que le routeur Wi-Fi qui permet aux utilisateurs d'accéder à internet, ne peut être qualifiée, à elle seule, de donnée à caractère personnel. En revanche, une adresse MAC peut être captée par des sites Internet lors de la navigation de l'Internaute, après que ce dernier se soit identifié. Une fois reliée à ces éléments d'identification, elle constitue nécessairement une donnée personnelle. C'est en fonction de tels éléments de contexte qu'il convient de décider si une adresse MAC peut être considérée, ou non, comme une donnée à caractère personnel* »[599].

300. Cette différence d'appréciation technique, volontaire ou non de la part de la société, est susceptible de diminuer l'intérêt de l'approche PbD. En tentant d'établir une norme technique de la protection de la vie privée, la PbD réduit le champ juridique à une définition

597 Traduction par l'auteur de: « *MAC addresses are simple hardware ID assigned by the manufacturer. And SSIDs are often just the name of the router manufacturer or ISP with numbers and letters added, though some people do also personalize them. However, we do not collect any information about householders, we cannot identify an individual from the location data Google collects via its Street View cars* » . Google Europe Blog, *Data collected by Google cars*, 27 April 2010, disponible sur https://europe.googleblog.com/2010/04/data-collected-by-google-cars.html (consulté le 01/09/17).

598 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2011-035 du 17 mars 2011 *prononçant une sanction pécuniaire à l'encontre de la société X*, Publiée sur Légifrance le 13 décembre 2016.

599 Ibid.

technique de la nature de la donnée et aux mesures de protections afférentes. Ce faisant, la PbD échappe aux analyses doctrinales qualifiant l'application du régime aux données à caractère personnel en s'appropriant le pouvoir normatif. Le risque est donc celui d'une requalification, à l'occasion d'un contrôle a posteriori de la nature de la donnée, donnant lieux à une sanction pouvant aller jusqu'à remettre en cause le modèle économique d'un service pour avoir négligé d'appliquer les protections nécessaires, tant au niveau juridique qu'au niveau technique.

301. Dans le cadre de notre exemple portant sur les répliques biométriques, il est certain qu'un industriel pourrait arguer d'une absence de qualification de celles-ci en tant que données biométriques, puisque par définition, celles-ci ne sont plus des données. La résultante serait un manque de protection adéquat, avec un risque pour la vie privée des personnes concernées. Toutefois, dans le cas d'une reconnaissance de l'application du régime, une seconde problématique apparait, précisément sur le niveau de protection adéquat à assurer autour de ces nouveaux objets. À ce jour, il n'existe aucune norme relative à la sécurité des répliques biométriques. Or, l'implication pratique et financière de la mise en place de protection est conséquente. Cela se traduit par la définition d'une méthode de stockage sécurisée, un suivi étroit du personnel avec la mise en place d'une procédure de contrôle de l'habilitation lors de la manipulation des répliques, un suivi de la destruction physique effective et une adaptation importante des droits des personnes concernées relatifs au droit d'accès ou d'opposition. Dans ce contexte, une différence d'appréciation de la protection applicable à ces données entre un responsable de traitement et les conclusions d'un contrôle de la CNIL a posteriori entraine des conséquences à plusieurs niveaux. Tout d'abord, les sanctions potentielles de la CNIL pesant sur les infractions au régime. Puis une transformation importante de la méthodologie du laboratoire effectuant ces recherches, tant au niveau des pratiques que de la physionomie des locaux ou des procédures d'habilitations. Eventuellement, une modification du modèle économique, puisque celui-ci dépend en partie des coûts de recherche et de développement.

302. C'est l'ensemble de la méthodologie de la PbD qui peut être remise en question. En encourageant les industriels à créer une forme de normalisation vis-à-vis de la protection technique de la vie privée dans l'innovation, elle introduit une forme d'homogénéisation des pratiques. En cas de revirement dans l'appréciation de celle-ci par une autorité indépendante,

cette normalisation fragilise l'ensemble de l'écosystème technique et économique. Il existe donc un risque issue de la dépossession normative qu'entraine la PbD per se.

2 – Le risque de dépossession normative porté par la PbD

303. Le développement de la PbD s'appuie sur la difficulté des responsables de traitement à traduire techniquement les implications du régime de protection des données à caractère personnel. Dans ce contexte, Ann Cavoukian propose à ces derniers de réfléchir eux-mêmes aux standards de protections, afin de mettre en place une protection technique de la vie privée globalisée[600]. Pourtant, selon Jean-Jacques Lavenue : « *Si l'affirmation classique du temps du droit à rebours du temps technologique est devenue un refrain répété ad nauséam pour fustiger les cadres législatifs et réglementaires, il demeure que des limites existent, des principes s'imposent. Beaucoup de ceux-ci sont suffisamment compréhensibles pour être traduisibles dans une technologie au prix d'un double effort : celui de vouloir les comprendre et celui de les intégrer* » [601].

304. Dans une telle perspective, l'intégration de la PbD au règlement général de protection des données apparait plus comme le don d'une fonction de normalisation à l'industrie que comme le renforcement des droits des citoyens Européens. En effet, à l'instar de la reconnaissance récente du droit à l'oubli par la Cour de Justice de l'Union Européenne[602], la PbD et la Privacy-By-Default[603] ne sont qu'une traduction technique du cadre législatif national et Européen. Le droit était jusqu'ici forgé par le législateur, en vertu de son pouvoir législatif, et par la jurisprudence en vertu du pouvoir judiciaire. Lorsque le cadre législatif nécessitait une précision, les différents organes fondateurs de la doctrine (G29, CNIL, Conseil d'Etat) établissaient conjointement et publiquement une politique d'appréciation de la licéité

600 Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, Ontario, Canada, December 2012, p2.

601 Lavenue Jean-Jacques, Codron Clémence, Desrumaux Nicolas, Hamerel Gaylord B., *Privacy By Design ou Privacy By Law*, Revue Droit international, Commerce, Innovation et Développement, n°2/2012, novembre 2012, Presses de l'Université de Bourgogne, p. 80.

602 CJUE gr. ch., 23 mars 2010, *Google Inc. V. Louis Vuitton Malletier Sa*., aff. C-236/08.

603Règlement (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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 25.

des procédures de traitement. Pourtant, selon l'article 25 paragraphe 3 du règlement général sur la protection des données, ce sera, dès 2018, à partir de la proximité du traitement avec les mesures recommandées par un mécanisme de certification que le respect des exigences juridiques seront définies.

305. Selon l'article 42 du règlement général sur la protection des données : « *les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération* »[604]. Cette certification sera assurée par des organismes privés. Bien que celle-ci n'exonère pas le responsable de traitement de toutes sanctions en cas d'infraction aux dispositions protection du régime, son respect définira son exposition juridique à celles-ci. Or, si le règlement charge les autorités de contrôle et le Comité de la mise en place des mécanismes de certification, il ne précise pas comment les certifications elles-mêmes seront éditées.

306. Dès lors, on peut penser que la définition de ces certifications sera en grande partie issue de l'industrie, comme on peut déjà l'observer avec la mise en place actuelle de codes de conduites pour certains secteurs informatiques. Ainsi dès 2015, les entreprises de Cloud Computing se sont dotées d'un code de conduite[605]. Celui-ci définit les pratiques du secteur relatives au régime protecteur des données à caractère personnel, mais plus encore, se veut être une base technique de discussion dans la cadre de la mise en place des futures certifications. Afin de lui assurer une sécurité juridique optimale, celui-ci fut communiqué au G29 afin d'obtenir un avis sur sa validité, et surtout, sur son devenir lorsque le regèlent général sur la protection des données entrera en vigueur. Bien que le G29 ne soit pas tenu d'analyser les codes de conduites, celui déclara: « *reconnaître le fait que ce Code apparait au moment d'une phase délicate de transition entre les différents régimes juridiques. Pour cette*

604 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 42.

605 Cloud Select Industry Group, *Data Protection Code of Conduct for Cloud Service Provider*, 19 January 2015.

raison, il paraît nécessaire de définir une stratégie de transition supervisée par une gouvernance structurelle, autorisant le code à être adopté et valide à travers ce processus, ainsi qu'au moment de l'adoption de la nouvelle régulation »[606]. Celui-ci va donc proposer un certain nombre de mesures destinées à assurer la licéité d'un tel code de conduite et sa survie dans l'environnement de normes certifiées lors de l'application du règlement général sur la protection des données. Ce faisant, le G29 participe activement, en se basant sur une proposition de l'industrie, à la future certification du secteur du Cloud Computing.

307. En utilisant avec intelligence les mécanismes mis en avant par la PbD, dont la certification est la clé de voute, l'industrie est capable d'influencer les normes techniques futures, et donc, les mesures de protection de la vie privée dans leur secteur. Il s'agit d'un basculement de la capacité normative du juridique vers le milieu économique et industriel à travers la procédure de certification.

Conclusion

308. Ainsi, en recourant à la PbD pour corriger les insuffisances du droit pour apprécier les structures techniques, le législateur Européen a opéré un basculement de la fonction normative au profit de l'industrie. Devenue elle-même rédactrice des règles qui lui seront imposées, celle-ci va disposer d'un atout considérable au regard des limites qui peuvent être fixées à l'exploitation des données et donc, à l'exploitation de la vie privée des personnes concernées.

309. Au final, ce nouvel environnement juridique incarné par le règlement général sur la protection des données[607] procède d'une volonté de défaussement de la responsabilité d'assurer l'existence des mécanismes de protection, allant du législateur à l'industrie.

606 Traduction par l'auteur de : « *The WP29 acknowledge the delicate phase of transition between legal frameworks within wich the Code applies. For this reason, it appears necessary to set up a transition management strategy, supervised by a real governance structure in place, allowing the code to be valid and effectively adopted throughout the transition and once the new Regulation is adopted* ». Groupe de Travail « Article 29 » sur la protection des données, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*, Adopted on 22 September 2015, 2588/15/EN, WP 232, p. 5.

607 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

Conclusion Partie I

310. La traduction matérielle du droit au respect de la vie privée dans l'innovation technologique s'est faite au prix de deux fragilités structurelles.

311. La première réside dans l'assimilation du droit des données à caractère personnel à l'autodétermination informationnelle[608], réduisant de fait une notion bien plus large à sa portion congrue, celle du périmètre offert à l'autonomie décisionnelle informationnelle. Ce faisant, le législateur a omis d'intégrer les aspects psycho-sociaux et leurs facteurs d'influence sur la capacité d'un être humain à se développer sereinement. La protection de l'individu face aux dangers du numérique bascule définitivement de la protection de sa vie privée à celle, bien plus réduite, de ses données à caractère personnel. Dans un monde où la numérisation systématique est devenue un indice de développement[609], cette faiblesse conceptuelle ouvre la voie vers une exploitation dangereusement libre des données issues de l'innovation numérique, à laquelle l'utilisateur pourra difficilement s'opposer.

312. La seconde correspond à la dimension technique de l'innovation. Face à un environnement transnational capable de s'opposer techniquement aux législations nationales, les législateurs Européens ont choisi de transférer le pouvoir de normalisation aux industriels afin d'intégrer avec une plus grande efficacité les mesures de protection à l'intérieur des produits numériques. Or, si les protections techniques ne sauraient être négatives par nature[610], la possibilité que l'industrie numérique définisse ces bornes est problématique de par le conflit d'intérêt qui en résulte. Ayant un intérêt économique à minimiser la protection et à exploiter intensivement les données, il est possible que celle-ci choisisse ses standards en fonction de ses intérêts. Ainsi, si l'on est capable de résoudre une partie de la problématique de l'applicabilité du droit dans l'innovation en recourant à la PbD, cela ne peut être un moyen de protection efficace si la fonction de normalisation est transférée dans son intégralité.

608 v. Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.
609 OECD, *Students, Computers and Learning, Making the Connection*, OECD Publishing, Paris, 2015.
610 v. Falque-Pierrotin Isabelle, *Déclaration publique en présence de la Commission des lois*, 14 décembre 2011.

313. Mais bien que différentes, ces deux fragilités structurelles relèvent de la même philosophie : celle d'un défaussement de la protection législative vers une protection individuelle. En réduisant la notion de vie privée numérique à celle de l'exploitation licite des données à caractère personnel, puis en plaçant l'individu au centre de cette condition de licéité, le régime a transféré la responsabilité d'évaluer l'impact d'un traitement sur un individu à l'individu lui-même. Dans ce système, l'individu serait alors tout puissant, capable de décider dans chaque cas les bornes du traitement relatif à ses données.

314. Si l'affirmation du législateur quant à cet état est vérifiée, alors la réduction conceptuelle amène une plus grande fluidité dans le contrôle des nouveaux moyens de l'innovation. Mais à l'inverse, si cela conduit à une surexploitation des conditions de licéité au détriment de l'individu, la réduction conceptuelle n'aura pas entrainé de bénéfice. Si nous avons démontré dans cette première partie les fragilités structurelles de la conceptualisation du régime, il nous reste à étudier ce qui peut faire ses forces en pratique : l'adaptation des acteurs de l'innovation à celui-ci.

Partie II

L'adaptation des acteurs de l'innovation au régime protecteur des données à caractère personnel

*

315. Comme nous l'avons vu précédemment, la protection de la vie privée dans l'innovation numérique a basculé d'une protection générale par le concept de droit au respect de la vie privée vers une simple protection des données à caractère personnel. Au centre de ce régime, le consentement devient donc l'outil principal de la licéité et du contrôle qu'un individu peut effectuer sur les traitements dont il est l'objet. Selon Christophe Lazaro et Daniel Le Metayer : « *on pourrait même affirmer qu'il constitue l'un des rouages fondamentaux de la mécanique juridique déployée par cette législation puisqu'il occupe la première place parmi les raisons légales autorisant un responsable de traitement à faire usage des données à caractère personnel* »[611].

316. Mais si le consentement est une raison régulièrement invoquée, il n'acquiert pas pour autant un statut différent des autres conditions de licéité. Pour le G29, le consentement n'annule pas « *les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie par la collecte des données excessive au regard d'une fin particulière* […] *Il s'agit en premier lieu d'une condition de licéité et non d'une renonciation à l'application d'autres principes* »[612].

611 Lazaro Christophe, Le Metayer Daniel, *Le Consentement au Traitement des Données Personnelles : une Perspective Comparative sur l'Autonomie du Sujet*, Revue juridique Thémis de l'Université de Montréal, voi.48 n°3, 2015, p. 765.

612 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du*

317. En suivant ce raisonnement, on pourrait conclure qu'il existe un nivellement des conditions cumulatives de licéité du traitement qui participe à la force du régime de protection dans son acception générale. Comme nous avons pu l'observer, celles-ci vont accompagner le traitement dans tout son développement temporel et matériel jusqu'à la destruction des données. Selon cette conception, la protection de la vie privée semble efficace en ne subordonnant pas l'ensemble de la protection au seul critère du consentement.

318. Toutefois, ce nivellement n'est qu'une illusion au regard de la temporalité de la définition de ces différents éléments. Par exemple, si la licéité est bien conditionnée à un critère de proportionnalité de la collecte, l'analyse s'appuie nécessairement sur ce qui a été exposée initialement à la personne concernée. Il en va de même pour les autres principes relatifs au traitement des données. La loyauté ou la transparence s'apprécient par rapport à la clarté de la procédure de recueil du consentement. De la même manière, l'adéquation, l'exactitude et la limitation des données collectées en fonction de la finalité est déterminée à partir de celle-ci. Ainsi, si le consentement n'est pas la seule condition de licéité, la procédure qui l'entoure est centrale. Pour paraphraser Orwell, on pourrait dire que si les conditions de licéité sont égales, le consentement est plus égal que les autres[613].

319. Cette structure juridique entraine un phénomène de cristallisation des enjeux de la licéité du traitement à l'intérieur d'une même procédure. Le consentement devient, par conséquent, le pilier juridique de l'économie numérique. Dans un tel contexte, l'intérêt des acteurs de l'innovation n'est plus de minimiser leur responsabilité en respectant scrupuleusement les conditions de licéité, mais de s'offrir une marge de manœuvre importante en termes d'acquisition et de valorisation des données grâce à une maitrise rédactionnelle de la procédure de recueil du consentement.

320. En termes de protection des individus, cela ne présente pas uniquement des désavantages. Selon Christiane Féral-Schul et Paul Christian : « *l'évolution qu'ont subie au cours de ces dernières années les droits au respect de la vie privée et à la protection des données à caractère personnel, […] s'apparentent de plus en plus à une exigence de libre*

consentement, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 8.

613 v. Orwell George, *La Ferme des Animaux*, Belin – Gallimard, 22 août 2013, 192 p.

épanouissement de la personnalité et à un désir d'autonomie individuelle. L'individu ne s'attend pas seulement à voir sa vie privée préservée de toute immixtion extérieure ; il revendique également la liberté de choisir et de contrôler les conditions dans lesquelles ses données personnelles peuvent être collectées et utilisées »[614]. Toutefois, certains opposent à cette vision idyllique l'idée que cette émancipation se fait au profit des industries numériques. En effet, comme l'observent Christophe Lazaro et Daniel Le Metayer : « *sur le plan empirique, certains auteurs font le constat d'un écart considérable entre théorie et pratique. Ainsi, les uns font fréquemment référence à l'inapplicabilité même d'une telle logique dans un contexte où les dispositifs techniques facilitent l'exploitation des données à l'insu des personnes. Les autres mettent en doute la possibilité d'un consentement véritablement éclairé et insistent sur les problèmes d'ordre informationnel et cognitif, notamment posés par le recours aux « politiques de vie privée » (Privacy policies)* »[615]. Dans les deux cas de figure, les conclusions sont identiques : le régime de protection se trouve atteint par la faiblesse du recours au consentement comme élément de licéité du traitement. D'un côté, celui-ci n'est pas suffisamment respecté, de l'autre, il n'est pas suffisamment bien défini.

321. Traduit dans sa dimension concrète, cela représente une forme de menace que fait peser l'innovation technologique sur la protection de la vie privée, à travers la manière dont celle-ci utilise l'exigence du consentement à ses propres fins. Nous devons analyser, par conséquent, dans quelle mesure la protection de la vie privée dans l'innovation numérique se fonde sur le consentement pour exister (Titre I) puis déterminer si une telle subordination a pour effet de fragiliser la protection (Titre II) en offrant aux responsables de traitement la possibilité d'exploiter les failles de cette procédure. À partir de ces observations, nous serons en mesure de déterminer de quelle manière les acteurs de l'innovation se sont adaptés au régime de protection.

322. À cette fin, nous poserons comme préalable le fait que la notion de consentement possède une validité binaire, positive ou négative. Par conséquent, nous ne retiendrons pas l'analyse de Christiane Féral-Schuhl et Christian Paul, qui font une distinction entre

614 Féral-Schul Christiane, Paul Christian, *Rapport d'information n°3119 sur le droit et les libertés à l'âge du numérique*, Déposé à l'Assemblée Nationale le 8 octobre 2015, p. 131.

615 Lazaro Christophe, Le Metayer Daniel, *Le Consentement au Traitement des Données Personnelles : une Perspective Comparative sur l'Autonomie du Sujet*, Revue juridique Thémis de l'Université de Montréal, voi.48 n°3, 2015, pp. 765-815.

consentement générique et consentement éclairé, qu'ils définissent comme suit : « *il convient […] de distinguer l'ensemble hétérogène de situations que peut recouvrir la notion générique de consentement – allant de l'accord tacite à la véritable manifestation de volonté – et le consentement véritablement éclairé, qui requiert une information particulière de l'utilisateur, mis en situation de mesurer les conséquences de son choix et d'accepter ou de refuser en toute indépendance le traitement de ses données* » [616]. En effet, une telle conceptualisation de la notion centrale de la licéité du traitement laisse supposer un affaiblissement du lien intime qui existe entre volonté et consentement. Comment, à partir de cet « *ensemble hétérogène* »[617], qualifier un respect uniforme de la volonté de la personne concernée ? Cela conduirait à une minimisation opportuniste de l'importance du consentement dans l'innovation numérique, en autorisant certains traitements à partir de procédures d'informations allégées, d'une manière incompatible avec les règlementations en vigueurs.

616 Féral-Schul Christiane, Paul Christian, *Rapport d'information n°3119 sur le droit et les libertés à l'âge du numérique*, Déposé à l'Assemblée Nationale le 8 octobre 2015, p. 138.
617 Ibid.

Titre I

Une protection liée au consentement de la personne

*

323. Selon Yves Poullet et Antoinette Rouvroy : « *le droit à la vie privée, nonobstant le fétichisme dont il est l'objet à la fois par le nombre de ses défenseurs les plus acharnés, et pour ses détracteurs les plus irréductibles, n'est rien d'autre qu'un instrument au service des capacités de développement personnel autonome, qui sont, dans une société donnée et à une époque donnée, nécessaires au fonctionnement démocratique du régime politique en vigueur* » [618]. En suivant cette logique, la technologie devient le medium de cette capacité développement personnel.

324. En cela, l'innovation technologique offre une opportunité pour l'individu de nouer de nouvelles relations, de s'informer ou même de s'exprimer avec une aisance jamais acquise jusqu'alors. Google nous permet de trouver tout type d'information avec une facilité déconcertante. Facebook nous met en relation avec des milliards de personnes. Et les différents services et produits disponibles décuplent les possibilités d'agir et d'échanger. Néanmoins, pour que ces nouveaux outils soient réellement bénéfiques, il est nécessaire que l'individu ait confiance dans la technologie, certain que celle-ci respectera sa volonté concernant les données qu'il sera amené à lui confier.

618 Poullet Yves, Rouvroy Antoinette, *Le Droit à l'Autodétermination Informationnelle et la valeur du développement personnel. Une Réévaluation de l'importance de la vie privée pour la démocratie*, Etat de Droit et virtualité, Ed. Karim Benyekhlef & Pierre Trudel, Montréal: thémis, 2009, p. 161.

325. Dans la première partie, nous avons observé comment ce constat permet de revenir à la définition holistique de la vie privée, en tant que condition d'existence d'une volonté individuelle à laquelle on associe un périmètre décisionnel, contribuant à donner à l'individu un contrôle et une certaine latitude dans l'exercice de cette capacité de développement. Nous avons cependant démontré que dans sa dimension concrète au cœur de l'innovation numérique, elle se transforme pour devenir le simple reflet de la volonté de l'individu lors de son utilisation de la technologie. Si dans la première partie nous n'avons pas pu étudier les conséquences de cette réduction conceptuelle quant à l'utilisation du régime qui peut en être fait par l'industrie, il nous appartient de le faire ici.

326. À cette fin, il faut commencer par reconnaitre que la technologie est portée en grande partie par des acteurs privés tels que les GAFA[619]. Par conséquent, l'innovation numérique est imprégnée du modèle économique dominant reposant sur des objectifs de valorisation des informations que les services vont chercher à obtenir de leurs utilisateurs. Selon ce modèle, en échange d'un accès gratuit à du contenu, le service obtient les données de l'utilisateur qu'il va ensuite traiter, puis vendre. C'est la concrétisation de l'adage « *si c'est gratuit, vous êtes le produit* ». À titre d'exemple, sur l'année 2015, Facebook a réalisé un bénéfice net en hausse de 25% s'établissant à 3.7 milliards de dollars[620], porté par la vente de publicité ciblée à destination de ses utilisateurs qui sont toujours plus nombreux.

327. C'est donc au cœur de ces échanges de données colossaux que l'analyse de l'efficacité de la protection de la vie privée va trouver un terrain fertile pour éprouver sa conception. Nous verrons dans un premier temps comment la notion de consentement est devenue centrale dans la collecte de données aux fins de valorisation (Chapitre I). Puis, nous observerons comment le consentement va se trouver détourné de son objectif initial, devenant un élément prépondérant dans les procédures traitements extensifs des données de l'utilisateur (Chapitre II).

619 Google, Amazon, Facebook, Apple.

620 Challenges.fr, *Facebook pulvérise ses bénéfices et son audience*, 28 janvier 2016, disponible sur http://www.challenges.fr/internet/20160128.CHA4405/facebook-pulverise-ses-benefices-et-son-audience.html (consulté le 01/09/2017).

Chapitre I

La place centrale du consentement dans la collecte des données

*

328. L'article 7 de la loi informatique et libertés intègre, comme élément préalable au traitement des données, la nécessité pour le responsable du traitement de recueillir le consentement de la personne concernée[621]. Ce consentement va ensuite lier le responsable de traitement aux finalités qu'il avait déclaré initialement. Pour cette raison, il est devenu indispensable pour les grands services internet de se doter d'une page expliquant en détails les traitements qu'ils vont appliquer aux données, ainsi que les éventuels procédures de valorisations auprès des annonceurs intéressés par celles-ci. En pratique, cela peut aller de la simple inscription à un annuaire en ligne à la commercialisation de ces données sur un autre service. Cependant, dans toute chaine de traitement, le consentement initial est le déclencheur.

621 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227*,* modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 7.

329. Des lors, en érigeant le consentement comme une valeur absolue de la légalité du traitement, le législateur a introduit dans la pratique un recours systématique aux conditions d'utilisation des services (Section I). À travers celles-ci, nous verrons que les GAFA sont en mesure de réaliser une captation extensive des données à travers l'exploitation du consentement par les nouveaux moyens de valorisation des données (Section 2), pratiques qui peuvent paraitre disproportionnées par rapport aux services rendus à l'utilisateur.

Section 1

La mise en place généralisée des conditions d'utilisation des services

330. En érigeant le consentement comme le principal fondateur de la licéité de la relation qui va s'établir entre un utilisateur et un service de l'innovation numérique, le droit impose la mise en place en amont d'une procédure de recueil du consentement systématique. Celle-ci doit être développée à la mesure du nombre d'utilisateurs et ne doit pas constituer une barrière à l'accession au service par une méthode qui serait trop contraignante. Ainsi, on peut comprendre que les services soient réticents à l'idée que l'inscription soit conditionnée à une demande préalable par lettre recommandée, nécessitant une signature sur les différentes informations relatives au traitement, telle que l'on pourrait exiger dans le cadre d'une vente immobilière par exemple. Dans leur objectif d'atteindre un maximum d'utilisateurs, l'inscription est une étape cruciale qu'il convient de rendre pratique : un processus trop compliqué pourrait freiner les velléités d'accès à un service.

331. Pour répondre à ce double objectif d'efficacité et d'accessibilité, les GAFA se sont progressivement dotés de conditions générales d'utilisation. Pages définissant avec plus ou moins de précision les traitements que vont subir les données des internautes, elles se réduisent généralement à une case à cocher qui va signifier la volonté de l'internaute à rejoindre le service sous certaines conditions d'utilisation des données.

332. Or, d'après le conseil d'Etat : *« Il est communément admis aujourd'hui que pour la grande majorité des services proposés sur les réseaux numériques, les modalités de recueil du consentement et d'information ne sont pas satisfaisantes. Les conditions générales d'utilisation (CGU) et les policies des sites internet relatives à la protection des données personnelles sont souvent très longues, écrites en termes techniques et difficiles d'accès ; elles sont en outre fréquemment modifiées. Il suffit souvent de cocher une simple case pour être réputé les avoir lues ; pour certains sites, la consultation ne constitue même pas un préalable pour l'accès au service, l'internaute ayant seulement la possibilité de cliquer sur le lien vers cette information* » [622]. Ce développement juridique des conditions générales de service est donc susceptible de fragiliser la protection de la vie privée.

333. Afin d'analyser ce phénomène, il nous faut d'abord comprendre comment le législateur a imposé indirectement ce recours systématique aux conditions générales de service (1). À partir de cette première observation, nous pourrons aborder les autres formes de légitimation des traitements, avec notamment la méthodologie qui a été appliquée aux cookies (2). Cette approche technologique mettra en avant la possibilité pour l'internaute de manifester son refus de voir ses données traitées indifféremment (3). Toutefois, les enjeux économiques de la valorisation balayent en grande partie ce type de technologie (4), ils encouragent un recours systématique au consentement, voire un renforcement de sa valeur pour légitimer les traitements (5).

622 Conseil d'Etat, *Etude annuelle 2014, Le numérique et les droits fondamentaux*, Doc. Fr, 2014, coll. Les rapports du Conseil d'Etat, p. 176.

1 – Une obligation juridique incontournable

334. Pendant le développement du régime applicable aux traitements des données à caractère personnel, le droit Français et le droit communautaire se sont accordés sur l'importance de la place du consentement de la personne[623]. Il constitue le préalable nécessaire au traitement, en l'absence de l'une des cinq catégories d'exceptions définies[624]. C'est un élément de légitimité fondamental pour le traitement, qui doit être donné « *expressément* » pour la loi Française[625], « *indubitablement* » pour la Directive 95/46/CE[626] et aujourd'hui de manière « *univoque* » avec le RGPD[627]. De plus, il doit être libre, spécifique et éclairé[628]. Or, s'il parait trivial à première vue, il devient dans l'innovation numérique le principal vecteur de sécurité juridique.

335. Dans un contexte de contractualisation croissante des relations dans le numérique à travers la mise en place généralisée des conditions de services, on aurait pu penser que l'exception présente à l'article 7 de la loi du 7 janvier 1978 s'applique ; utilisant l'existence d'un contrat entre la personne concernée et le responsable de traitement pour supprimer le principe du consentement préalable au traitement. Mais pour celle-ci, seul l'objectif contractuel strict doit être entendu. Ainsi : « *un responsable de traitement se fondant sur l'article 7, point b), dans le cadre de la conclusion d'un contrat ne peut en faire un usage*

623 On retrouve la notion de consentement à l'article 7 Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227, ainsi que dans l'article 7 de la Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

624 « *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : 1° Le respect d'une obligation légale incombant au responsable de traitement ; 2° La sauvegarde de la vie de la personne concernée ; 3° L'exécution d'une mission de service public dont est investi le responsable de traitement ; 4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; 5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaitre l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ». Article 7 de la loi n° 78-17 du 6 Janvier 1978, *relative à l'informatique, aux fichiers et aux libertés*, art. 1 JORF 7 Août 2004.

625 Ibid. Article 8.

626 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, Article 7.

627 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 4.

628 Ibid.

extensif pour justifier le traitement de données au-delà de ce qui est nécessaire, pour ce faire, il devra justifier le traitement supplémentaire par un consentement spécifique »[629]. C'est donc dans les éléments contextuels du traitement que va se loger la licéité de celui-ci, en le limitant strictement à l'exécution des obligations contractuelles.

336. Cette exception s'applique également à la période précontractuelle « *pour autant que les démarches soient accomplies à la demande de la personne concernée, plutôt qu'à l'initiative du responsable du traitement ou d'un tiers. Par exemple, si une personne demande à un détaillant de lui faire une offre de prix pour un produit, le traitement de données effectué à cette fin, tel que la conservation, pour une durée limitée, de l'adresse et des informations à propos de ce qui est demandé, pourra s'appuyer sur ce fondement juridique* » [630]. Appliquée aux techniques de valorisation des données utilisateurs que nous avons exposées dans notre introduction, cette exception aurait pu justifier des traitements extensifs des données.

337. Néanmoins selon le G29, le contrat passé entre l'utilisateur et le service au moment de son inscription « *ne peut pas servir de fondement juridique pour établir un profil des goûts et du mode de vie de l'utilisateur à partir de son historique de navigation sur un site internet et des articles achetés. En effet, le responsable du traitement des données n'a pas été chargé, dans un contrat, d'établir un profil mais de fournir des produits et des services par exemple. Même si ces activités de traitement sont expressément mentionnées en petit caractère dans le contrat, elles n'en deviennent pas pour autant « nécessaires » à l'exécution de ce dernier* » [631]. En conséquence, ce type d'exception ne peut pas être invoqué dans le cadre de la valorisation des données personnelles. Il faudra nécessairement établir une procédure de recueil du consentement distincte concernant l'utilisation des données personnelles traitées.

338. De manière dématérialisée, cette étape requiert du responsable de traitement la rédaction d'un texte qui détaille ces informations pour les présenter sur l'écran de l'utilisateur. À la lecture de celles-ci, la personne doit s'estimer suffisamment informée pour donner un consentement valide et explicite. Généralement présentée sous la forme d'un double clic à

629 Ibid.

630 Groupe de Travail « Article 29 » sur la protection des données, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, adopté le 9 avril 2014, 844/14/FR, WP 217, p. 20.

631 Ibid, p19.

effectuer[632], la procédure est enregistrée par le responsable de traitement qui doit la conserver pendant toute la durée du traitement des données. D'autres techniques peuvent être utilisées, comme par exemple « *des fenêtres pop-up que le consommateur accepte au fur et à mesure de son utilisation du service* »[633]. Cependant, « *l'utilisation répétée de fenêtre pop-up peut agacer le consommateur au point où il ne regarde plus les messages et les accepte systématiquement* »[634], affaiblissant la valeur de son consentement. De manière pratique, les conditions générales semblent donc la façon la plus simple d'acquérir le consentement, sans gêner pour autant la navigation.

339. Cette étape peut porter sur des documents aux dénominations diverses: les conditions générales de services, les conditions et règlements d'utilisation, les règles de confidentialité, etc. Le seul dénominateur commun reste celui de la manifestation de volonté expresse à l'utilisation des données qui y est demandée, et à laquelle l'une des clauses doit faire référence. Peu importe la forme ou le nom que va porter cette procédure dans les faits, elle emporte l'engagement contractuel et matérialise le consentement dès lors que les informations sur le traitement des données sont indiquées de manière adéquate. En donnant son consentement, la personne devenue utilisatrice du service accepte expressément l'ensemble des traitements qui y sont détaillés.

340. Ces règles de confidentialités sont finalement le produit de la nécessité de recueillir le consentement d'une manière sûre et pratique. En érigeant cette exigence, le législateur a donc imposé indirectement un recours systématique aux conditions d'utilisations et aux règles de confidentialité sur les services numériques. Celle-ci va s'imposer à la majorité des services dématérialisés que l'on peut trouver sur internet, qu'il s'agisse d'un service de messagerie, d'un service de vente en ligne ou simplement d'un réseau social.

341. La raison principale tient dans un fait : l'innovation numérique peut difficilement se passer de la valorisation des données, principal carburant de son économie. Lorsque l'on observe la liste des sites internet les plus visités en France, on trouve le service de recherche

632 D'une manière générale, le premier clic consiste en la sélection d'une case : « *j'ai lu et j'accepte les conditions générales de service* », avant d'accepter l'inscription par un second clic.

633 Féral-Schul Christiane, Paul Christian, *Rapport d'information n°3119 sur le droit et les libertés à l'âge du numérique*, Déposé à l'Assemblée Nationale le 8 octobre 2015, p. 273.

634 Ibid. p274.

en ligne Google, le service de vidéo à la demande Youtube, le service de réseau social Facebook, ou le site de vente entre particuliers Leboncoin.fr[635]. Ces services sont tous gratuits d'accès. Ils ne nécessitent pas l'achat d'une application ni un abonnement mensuel au service.

342. Le modèle économique est celui de la valorisation des données des internautes. En collectant et en traitant les données, les services de l'innovation numérique sont capables de proposer à des annonceurs un affichage ciblé des publicités en fonction des différents centres d'intérêts de l'internaute. La possibilité d'afficher une offre ciblée à un internaute susceptible d'être intéressé, voir même de pouvoir individualiser l'annonce, recèle une valeur importante que le service s'octroie en traitant la donnée[636]. Dès lors, le consentement au traitement devient indispensable afin de valoriser les données. Lors de l'étape de création d'un compte, il sera donc précisé les traitements de données opérés par le responsable, notamment en ce qui concerne la possibilité de tirer un profit économique des données qui seront collectées.

343. Cette étape peut même intégrer d'autres informations qui ne sont pas directement liées au service. En 2015, presque un tiers du trafic internet était généré par le mobile[637]. Les applications mobiles vont alors capter non seulement les informations que l'utilisateur va produire en utilisant le service, mais également certaines informations disponibles sur le téléphone, comme les contacts, les Short Message System (SMS) etc. Dans ce nouvel environnement technologique porteur d'une pluralité de moyens d'accès, la mise en place d'une modalité d'inscription unique, incluant l'acceptation des conditions d'utilisations, devient donc la norme.

344. La combinaison de ces éléments juridiques et techniques va fonder une mise en place généralisée des conditions générales de service. Toutefois, on peut trouver au moins une exception à cette obligation de recueillir le consentement au préalable : les cookies de mesure d'audience.

635 Alexa, Top Sites In France, site internet d'Alexa, disponible sur http://www.alexa.com/topsites/countries;0/FR, consulté le 20/03/2016.

636 v. Babinet Gilles, *L'Ere Numérique, Un Nouvel âge de l'Humanité : Cinq Mutations Qui Vont Bouleverser Notre Vie*, Le Passeur éditeur, janvier 2014, 236 p.

637 We Are Social, *Digital, Social and Mobile* 2015, WeAreSocial, disponible sur http://wearesocial.com/fr/etudes/digital-social-mobile-les-chiffres-2015 (consulté le 01/09/2017).

2 – Une exception technique : les cookies de mesure d'audience

345. Le principe du recueil préalable du consentement n'est pas systématiquement applicable à tous les traitements qui ont lieux sur internet. Il existe une exception notable, celle applicable aux technologies de mesure d'audience. Autrement appelés Cookies[638], ces outils sont des fichiers placés sur le disque dur de l'internaute par le site internet visité. Ils sont présents sur la majorité des pages internet, et représentent l'un des enjeux technique et économique déterminant de l'industrie numérique[639]. Cette technologie permet au service de reconnaitre l'utilisateur lorsqu'il se connecte sur la plateforme, de stocker des informations sur ses habitudes de navigation, de lui associer des présentations personnalisées ou des publicités en fonction de ces goûts. À chaque fois que l'utilisateur naviguera de nouveau sur le site, le service aura la possibilité de lire ces informations pour lui restituer ses préférences en fonction de son historique. Les régies publicitaires numériques s'appuient sur cette technologie et ont développé des programmes informatiques qui peuvent être intégrés de manière transparente dans les pages web. Implantées en grand nombre sur la toile, elles monnayent ensuite les informations recueillies auprès d'annonceurs. Pour autant, ce n'est pas la seule possibilité qu'offre l'utilisation des cookies.

346. Un cookie donne l'opportunité à un site internet de mesurer le temps de visite et de faire la distinction entre les différents internautes pour obtenir des statistiques affinées sur la pertinence et l'audience des différentes pages de son service. L'objectif n'est pas de valoriser économiquement ces informations, mais d'améliorer la qualité du service et la pertinence des articles ou des services proposés à la navigation. C'est cette seconde utilisation qui constitue une exception au régime général applicable au traitement des données.

638 Selon la CNIL : "*Sont concernés les traceurs déposes et lus par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé tells qu'un ordinateur, un Smartphone, une liseuse numérique et une console de jeux vidéo connectées à internet*". Commission Nationale de l'Informatique et des Libertés, « *Cookies & Traceurs : que dit la loi ?* », Non daté, disponible sur https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi (consulté le 01/09/17).

639 Gayat Pascal, *Blocage des Cookies, Quels Enjeux pour le Marketing à la Performance ?*, Journal du net, 29 mars 2013, disponible sur http://www.journaldunet.com/ebusiness/expert/53814/blocage-des-cookies--quels-enjeux-pour-le-marketing-a-la-performance.shtml (consulté le 01/09/19).

347. Intégrées au régime juridique par l'adoption de la directive 2009/136/CE[640], et par l'ordonnance n°2011-1012 du 24 août 2011[641] relative aux communications électroniques qui a transposée la directive, ces technologies peuvent, dans des conditions définies et restreintes, se passer du consentement. Pour cela, il faudra que l'éditeur du site délivre une information claire et complète sur la présence de ces cookies, qu'un mécanisme d'opposition soit accessible simplement, que les données collectées ne soient pas recoupées avec d'autres traitements, que le cookie serve uniquement à la production de statistiques anonymes, qu'il ne suivent pas la navigation de l'internaute sur d'autres sites, que l'adresse IP permettant la géolocalisation ne soit pas plus précise que l'échelle de la ville, et que cette traçabilité ne soit pas supérieure à 13 mois à compter de la première visite.

348. Cependant, de l'avis de la CNIL elle-même « *peu d'outils permettent de respecter ces différentes conditions* » [642]. Ces conditions semblent trop restrictives alors que la majorité des sites internet s'appuie sur ces cookies pour créer de la valeur avec les données. Le régime général est donc applicable dans la plupart des cas, et le recueil du consentement est nécessaire. La difficulté sera d'adapter cette nécessité à une technologie qui est présente sur chaque page internet et qui constitue, sans être totalement indispensable, l'une des briques technologiques génériques de la navigation.

349. Le résultat de cette confrontation s'est traduit par la communication de la CNIL sur les Cookies datée du 16 décembre 2013[643], rappelant l'importance du consentement et donnant des pistes pratiques pour introduire cette obligation juridique dans les sites internet. L'objectif principal était de pouvoir conserver une certaine fluidité de navigation, tout en donnant la possibilité à l'internaute de signifier son acceptation ou son refus.

---

640 Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009, *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal Officiel de l'Union Européenne n°L337/11, 18 décembre 2009.

641 Ordonnance n°2011-1012 du 24 août 2011 *relative aux communications électroniques*, JORF n°0197 du 26 août 2011, p. 14473 texte n°49.

642 Commission Nationale de l'Informatique et des Libertés, « *Cookies & Traceurs : que dit la loi ?* », Non daté, disponible sur https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi (consulté le 01/09/17).

643 Commission Nationale de l'Informatique et des Libertés, « *Recommandation sur les cookies : quelles obligations pour les responsables de sites, quels conseils pour les internautes ?* », 16 décembre 2013.

350. En accord avec la solution proposée par la CNIL, on a donc vu fleurir sur les sites internet des bandeaux expliquant la présence de ces dispositifs. Ceux-ci doivent informer l'internaute et rediriger vers une page expliquant à l'utilisateur comment paramétrer ses cookies. La CNIL a mis à disposition sur sa plateforme un modèle de bandeau à destination des services[644]. Il s'agit d'un petit texte encadré indiquant que « *en poursuivant votre navigateur sur ce site, vous acceptez l'utilisation de [Cookies ou autres traceurs] pour vous proposer [Par exemple des publicités ciblées adaptés à vos centres d'intérêts] et [Par exemple, réaliser des statistiques de visites]* »[645]. Celui-ci sert à informer l'internaute de manière optimale, tout en lui donnant la possibilité de refuser de continuer la navigation sous ces conditions.

351. La Commission impose également une information pratique sur les possibilités de s'opposer techniquement au dépôt de cookie sur son terminal. Grace à cette seconde information, l'utilisateur aura la possibilité d'obtenir des détails techniques sur le fonctionnement des cookies et sur les paramètres de son navigateur permettant de bloquer leurs dépôts ou utilisations. L'internaute est alors acteur de sa propre protection et ses choix techniques sont imposés aux services. Pour autant, la valeur de cette action technique ne peut se mesurer que devant la capacité de l'internaute à manifester le refus de ce suivi, et à ce que celui-ci soit pris en compte par les services.

3 – La manifestation technique du refus de suivi de l'internaute

352. Sur le plan technique, il existe différentes solutions permettant à l'internaute de manifester son choix face à la mise en place de cookies sur sa propre machine[646]. Celui-ci peut désactiver temporairement ou supprimer définitivement les cookies présents sur son navigateur afin d'éviter de se faire reconnaitre par un service donné. Pour cela, il faudra bien évidemment commencer par se déconnecter de ses comptes, et relancer une session vierge. En

644 Commission Nationale de l'Informatique et des Libertés, « *Exemple de Bandeau Cookies : comment recueillir valablement le consentement des internautes aux cookies et traceurs de votre site ou application web ?* », 30 décembre 2015, site internet de la CNIL, https://www.cnil.fr/fr/exemple-de-bandeau-cookie (consulté le 01/09/17).

645 Ibid.

646 Pour un exemple de gestion des cookies sur le navigateur Firefox, v. MacFarlane Nigel, *Firefox à 200%*, O'Reilly, 7 Juillet 2005, 194 p.

arrivant sur son site habituel, le service ne sera pas en mesure de lire d'éventuels cookies installés préalablement, et attribuera automatiquement une identité neuve à l'internaute. Cette procédure est d'ailleurs l'une des solutions prônées par les experts informatiques pour éviter de faire face aux procédés de « *yield management*» [647] basés sur l'IP Tracking des sites de vente de billets en ligne[648]. En l'espèce, certains sites internet retiennent que l'internaute est intéressé par une offre lorsqu'il en examine une, et lors de sa seconde visite, il propose un prix légèrement supérieur pour susciter l'urgence dans l'achat. Décelant dans ces pratiques une atteinte potentielle, la CNIL s'est penchée sur ce genre de pratique avec la DGCCRF[649]. L'une des constatations était notamment que les opérateurs basaient le prix proposé « *en fonction du site précédemment consulté par l'internaute* » [650], et a décidé de poursuivre ses investigations.

353. Face à ces pratiques commerciales, la limitation technique appliquée aux cookies protège l'internaute. Toutefois, cette procédure peut être contraignante selon les terminaux utilisés. Afin de réduire celle-ci, les navigateurs récents ont mis en place une option permettant de réduire la difficulté technique à une simple case à cocher.

354. Généralement nommé « *navigation privée* »[651], l'activation de cette option permet à l'internaute de naviguer sans que soient lus les cookies présents sur son ordinateur. En cas de dépôt, ceux-ci seront automatiquement effacés lors de la fermeture de la cession. Cette procédure autorise l'ouverture d'une cession vierge lors de chaque navigation qui ne prendra pas en compte l'historique de navigation antérieur. Sans nécessiter des connaissances approfondies en informatique, cette option est facilement accessible.

---

647 « *Le yield management est une technique marketing de tarification flexible utilisée dans les services caractérisés par une forte présence de couts fixes et par une certaine inertie des capacités proposées (transport en commun, hôtellerie, ...). Le yield management consiste à maximiser le chiffre d'affaire généré en jouant sur les variables de prix et le coefficient d'occupation à l'aide d'une politique de tarification différenciée* ». Bathelot Bertrand, *Définition Yield Management*, Définition Marketing, l'Encyclopédie illustrée du marketing, 16 Mai 2015, disponible sur http://www.definitions-marketing.com/definition/yield-management/ (consulté le 01/09/2017).

648 Calixte Laurent, *Billets d'avions : comment échapper à l'IP tracking des compagnies aériennes*, Challenges, 12 juin 2013, disponible sur http://www.challenges.fr/entreprise/20130612.CHA0739/billet-d-avions-comment-echapper-a-l-ip-tracking-des-compagnies-aeriennes.html (consulté le 01/09/2017).

649 Commission Nationale de l'Informatique et des Libertés, *IP Tracking : conclusion de l'enquête conjointe menée par la CNIL et la DGCCRF,* 27 Janvier 2014.

650 Ibid.

651 Voir le site internet de Mozilla Support pour Firefox pour un exemple de cette option sur un navigateur, https://support.mozilla.org/fr/kb/navigation-privee-naviguer-avec-firefox-sans-enregistrer-historique, (consulté le 01/09/2017).

355. Mise en place par les éditeurs de navigateurs internet, elle constitue l'une des briques de la protection du droit au respect de la vie privée sur internet sur le plan technique. En donnant la possibilité à l'internaute de masquer tout ou partie de son identité, cette option constitue une première ligne de défense en faveur du respect du consentement de la personne dans le traitement des données à caractère personnel. Lorsque que l'option est activée, l'internaute redevient quasiment un simple anonyme pour les sites sur lesquels il va effectuer sa visite[652]. Son cheminement ne sera pas enregistré sur sa machine et cela n'affectera ses futures visites lors de la réactivation des cookies. Cependant, en aucun cas, l'activation de l'option « *navigation privée* » peut constituer une protection suffisante face aux différentes technologies de traçages disponibles sur les réseaux. Celle-ci ne modifie pas l'adresse IP, servant pour de nombreux services à reconnaître l'individu, et qui est reliée à l'adresse physique de la ligne, ni l'adresse MAC de l'ordinateur qui identifie le terminal de façon unique. En somme, elle constitue simplement un frein à l'utilisation des données et à la collecte de ses informations, ainsi que la possibilité d'une parenthèse dans le suivi qui est effectué de l'internaute lors de ses pérégrinations numériques.

356. L'un des défauts de l'option « *navigation privée* » est notamment de ne pas constituer réellement un message à destination des tiers. Du point de vue du service, l'interprétation de ces modifications n'apparaît pas clairement. D'une part, le refus technique au dépôt des cookies peut trouver sa cause dans un problème de configuration, ou simplement une incompatibilité dans les différents programmes et langages informatiques utilisés. D'autre part, il ne s'agit pas d'un refus exprès. Il fallait donc trouver un moyen de pouvoir envoyer un message clair au service pour manifester son refus avant le déploiement des cookies sur la machine.

357. Dans cette optique, la recherche en informatique est venue soutenir le droit en essayant d'exprimer techniquement la manifestation du refus à l'utilisation des cookies[653]. Appelée

652 La navigation n'est pas pour autant intraçable, pour une définition technique plus complète, v. Untersinger Martin, *Anonymat sur internet : Protéger sa vie privée*, Editions Eyrolles, 29 octobre 2014. 264 p.

653 Shwartz Ari, Sherry Linda, Cooper Mark et al. Message to Donald S. Clark, Secretary of the Federal Trade Commission, *In advance of the FTC Town Hall, "Ehaviorial Advertising: Tracking, Targeting, and Technology",* to be held November 1-2, 2007 in Washington DC. Center for Democracy & technology.

« *Do Not Track* »[654] et soutenue par le W3C[655]. Cette technologie consiste en l'activation d'une option indiquant au site internet visité le refus du suivi de l'internaute en ce qui concerne les cookies. Cela permet d'indiquer de façon expresse au site web que l'internaute refuse par avance tout type de cookies. Pour que cette innovation soit prise en compte, il fallait un investissement des principaux éditeurs pour qu'ils reconnaissent l'existence de ce procédé, et l'intègre au sien de leurs technologies. Cette introduction s'est donc réalisée progressivement, avec le soutien du W3C et certains géants de l'internet jusqu'en 2012, date à laquelle les principaux acteurs numériques se sont engagés en sa faveur[656]. Depuis, la plupart des grands services informatiques se sont ralliés à cette technologie, jusqu'à en faire la promotion et l'intégrer à leurs outils. Microsoft a ajouté cette option dans son navigateur grand public internet explorer[657], de même que Mozilla, Apple et Google[658].

358. Cependant pour la plupart des navigateurs, cette option n'est pas activée par défaut. Elle nécessite encore une action de la part de l'utilisateur pour être indiquée aux tiers. De plus, comme le souligne le rapport *Consumer Data Privacy in a Networked World* de la Maison Blanche: « *Ceux-ci requiert des développements plus approfondis afin de s'assurer de la facilité d'utilisation, de l'équilibre vis-à-vis de l'utilisation des données personnelles, de l'intérêt de la sécurité publique, et présenter au consommateur une vision claire des potentiels couts et bénéfices liés à la limitation de la collecte de ses données* »[659]. Enfin, l'un des éléments qui peut être mis en avant, et le fait qu'à ce jour, aucune législation ne vient

654 Traduction de : « *Ne pas suivre* ».

655 Dans cette optique, le World Wide Web Consortium a décidé de se doter d'un groupe de travail dédié à la consolidation et à la promotion de cette technologie : le Tracking Portection Working Group. Celui-ci se définit comme suit: "*The Tracking Protection Working Group is chartered to improve user privacy and user control by defining mechanisms for expressing user preferences around Web tracking and for blocking or allowing Web tracking elements. The group seeks to standardize the technology and meaning of Do Not Track, and of Tracking Selection Lists*". Site du W3C, Tracking protection working Group, disponible sur https://www.w3.org/2011/tracking-protection/. (consulté le 01/09/2017).

656 Reitman Rainey, *White House, Google and Other Advertising Companies Commit to Supporting Do Not Track*, Electronic Frontier Foundation, 23 February 2012, disponible sur https://www.eff.org/fr/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track (consulté le 01/09/17).

657 Microsoft, *Utiliser la protection contre le tracking dans internet explorer,* site internet de Microsoft, site internet de Microsoft, disponible sur http://windows.microsoft.com/fr-fr/internet-explorer/use-tracking-protection#ie=ie-11 (consulté le 01/09/2017).

658 L'option Do Not Track est présente dans les navigateurs Firefox, Safari et Chrome depuis 2012.

659 Traduction par l'auteur de: « *They require further development to ensure they are easy to use, strike a balance with innovative uses of personal data, take public safety interests into account, and present consumers with a clear picture of the potential costs and benefits of limiting personal data collection* ». The White House, *Communication: Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington, February 2012, p. 13.

mentionner le non-respect de la prise en compte de cette technique, bien que le G29 se soit prononcé en sa faveur.

359. Le G29 recommande aux sites internet de prendre en compte ce choix et de le considérer comme un refus à l'utilisation de ces technologies de suivi[660]. Mais aucun contentieux n'a été constaté depuis cette communication, et il n'en est fait aucune mention dans le règlement Européen sur les données à caractère personnel[661]. La mise en place d'un cadre juridique protecteur de ce choix dans les options de son navigateur serait pourtant l'une des solutions permettant un plus grand respect de la volonté des utilisateurs.

360. Cette absence pourrait s'expliquer par deux phénomènes. Tout d'abord, il existe une difficulté inhérente à la promotion d'une technologie particulière, au risque de la voir défaillir et tomber en désuétude. En faisant entrer dans la norme juridique une norme technique, on lie la pertinence de la première au destin de la seconde. Ensuite, les informations présentes dans les cookies ne sont plus porteuses de la valeur la plus intéressante pour les services et par défaut, le passage par la signature des conditions générales de service vient contrer l'option « *Do Not Track* ».

4 – Une nécessité économique

361. À la lumière de nos précédentes observations, il résulte que dans la plupart des cas, les conditions générales de service sont indispensables pour les services numériques existants. Ces derniers n'ont pas pour objectif d'effectuer des mesures d'audience, alors qu'ils pourraient bénéficier de l'exception au consentement, mais bien de recouper et de traiter de façon économique les données recueillies. Pour cela, ils ont besoin de capter un maximum d'information et les cookies ne deviennent plus qu'un lot de données parmi d'autres. La raison principale, tient dans ce qui fait l'essence même de l'économie d'internet : la valorisation des données à caractère personnel. Selon Meglena Kuneva, la Commissaire

660 Groupe de Travail « Article 29 » sur la protection des données, *Opinion 04/2012 on Cookie Consent Exemption*, adopted on 7 June 2012, 00879/12/EN WP 194.

661 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

Européenne à la consommation: « *Internet est un service porté par la publicité et le développement des techniques de marketing basées sur l'identification et les données personnelles. Les données personnelles sont le nouveau pétrole d'internet et la nouvelle monnaie du monde numérique* » [662].

362. Il en va de l'intérêt des services d'exploiter ces données et par conséquent, l'exception qui s'applique à une catégorie précise de cookies n'a que très peu de cas concrets d'utilisation. Le service cherchera donc toujours à étendre sa capacité de captation et mettra en place des conditions générales de service. Avec le recueil du consentement, le responsable du traitement s'assure de la pérennité de son modèle économique et celui vient nullifier l'activation de l'option « *Do Not Track* » à travers l'action positive de l'utilisateur lorsqu'il accepte les règles de confidentialité à posteriori de son activation. En ayant à l'esprit que la plupart des grands sites internet possèdent aujourd'hui ce type de clause, on peut donc se poser la question de la survie, ou du moins, de la reconnaissance juridique future de l'option « *Do not Track* ».

363. Les opérateurs de services intègrent ces conditions dès les premiers pas sur leurs sites internet et leur intérêt n'est pas de reconnaitre une telle option. En étant au cœur du modèle économique, la valorisation doit s'appuyer sur une manifestation de volonté expresse de la personne pour atteindre une sécurité juridique optimale. En cas de manquement, les sanctions civiles et pénales sont directement applicables et peuvent toucher à la viabilité de l'entreprise, ainsi que nous l'avions observé dans la première partie de cette étude. De plus, si l'on considère que le traitement est qualifié dès la collecte des informations, toute entorse au régime de protection s'applique non seulement au traitement lui-même, mais également à toute utilisation ultérieure des données. Dans son arrêt daté du 25 Juin 2013, la chambre commerciale de la Cour de Cassation considérait que la vente d'un fichier de données à caractère personnel qui n'avait pas été déclarée à la CNIL constituait une vente d'objet illicite[663]. En déclarant nulle la vente de ce fichier, la Cour de Cassation ferme la voie à toute

662 Traduction par l'auteur de: « *Internet is an advertisement supported service and the development of marketing based on profiling and personal data is what makes it go round. Personal data is the new oil of the internet and the new currency of the digital world* ». Meglena Kuneva, *Déclaration publique lors de la Roundtable on Online Data Collection, Targeting and Profiling*, Brussels, 31 March 2009.

663 Cass. Com., 25 juin 2013, n°12-17037, Bull. Com. 2013, IV, n°108.

tentative de vente de donnée à des tiers, et par corollaire, touche une grande partie de l'économie des services numériques qui sont basés sur l'exploitation publicitaire.

364. En considérant ceci, l'avenir du régime entourant la captation des données pourrait prendre appuis sur une technologie « *Do Not Track* » à la seule condition que celle-ci intègre d'une manière plus complète les différentes données, au-delà des cookies, que l'utilisateur veut autoriser le service à capter. En détaillant les différents type de données, telles que les mouvements de la souris, la vitesse de frappe ou d'autres éléments, ce nouveau régime pourrait constituer un socle technique pour que chaque personne puisse définir les données quelle souhaite partager. Les règles de confidentialités et autres textes ne seraient plus qu'une information sur les traitements exacts que les données autorisées par l'utilisateur subiront en fonction des services. Cependant, cela viendrait toucher directement à la manne économique sur laquelle se base les services pour exister.

365. Au-delà de cet aspect économique, le débat légal réel qui entoure la reconnaissance et l'adoption de cette technologie se concentre sur le moment où l'on place la reconnaissance juridique de l'expression de la volonté de l'internaute. Est-il possible de manifester un refus anticipé au traitement, qui nullifiera ensuite le consentement aux conditions générales ? Ou bien le consentement pris en compte est-il toujours celui donné à posteriori aux conditions générales ? En l'absence d'une reconnaissance législative forte de la première option, il y a fort à parier que seule la seconde sera reconnue par les tribunaux.

5 – vers un renforcement de la valeur du consentement lié aux règles de confidentialité

366. L'objectif assumé du règlement Européen est de sécuriser les investissements dans le numérique en renforçant la valeur du consentement[664]. Choix assumé en faveur d'un renforcement du formalisme, la proposition de règlement sur les données à caractère personnel a souhaité préciser les conditions entourant cette pratique dans son article 7[665] en

664 v. Commission Européenne, *Communiqué de Presse*, IP/12/558, Bruxelles, 4 Juin 2012.

665 Commission Européenne, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[First Reading],* Brussels, 15 December 2015.

renforçant son caractère univoque. Selon la version définitive publiée le 27 avril 2016, le consentement « *devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et unique son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètre techniques pour des services de la société de l'information ou au moyen d'un autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel* » [666].

367. Toute infraction à ces éléments aura pour effet de rendre le consentement nul. En cas de conflit, ce sera au responsable de traitement d'amener la preuve du recueil conforme du consentement[667]. L'intérêt est de préciser les conditions dans lesquelles le consentement est recueilli afin de sécuriser les investissements. Selon la Commission : « *un cadre législatif solide, clair et uniforme au niveau de l'Union contribuera à libérer le potentiel du marché unique numérique et à promouvoir la croissance économique, l'innovation et la création d'emplois* » [668]. Pour cette raison, nous devrions observer un renforcement et un recours systématique aux conditions générales de services.

368. En conséquence, la présence de ces conditions générales de services devrait s'étendre à l'ensemble des sites et des services existants dès lors qu'ils traitent les données des utilisateurs. Si certains étaient dans l'illégalité, en leur absence ou par leurs manques de clartés, les précisions apportées aux exigences de formalisme et d'informations viendront renforcer le régime de protection. Certains services ont déjà fait l'objet de sanction par la CNIL pour leurs manques de lisibilités. Ainsi, le 3 Janvier 2014, la Commission nationale prononçait une sanction de 150 000 € à l'encontre de Google pour un défaut de conformité de

666 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, considérant 32.

667 Ibid. Article 7.

668 Commission Européenne, *Communication de la Commission au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions, Protection de la vie privée dans un monde en réseau : un cadre européen relatif à la protection des données, adaptés aux défis du 21e siècle*, IP 2012/9, Bruxelles, le 25 janvier 2012, p. 9.

ses règles de confidentialité[669]. D'après l'autorité indépendante, la société n'informait pas suffisamment les utilisateurs sur les conditions et les finalités de traitement des données. Celle-ci ne se conformait pas aux obligations nécessaires de recueil de consentement préalablement au dépôt de cookies sur les terminaux des internautes et, enfin, la société procédait, sans base légale, à la combinaison de l'intégralité des données pour l'ensemble de ses services.

369. En rappelant ces exigences dès 2014, la CNIL préparait le terrain pour le prochain règlement Européen en matière de données à caractère personnel, et confirme l'attention que portent les organismes de contrôle aux règles de confidentialités qui sont devenues aujourd'hui indispensables pour chaque service. Ceci renforce l'importance des critères de validité du consentement, ainsi que son rôle central dans la valorisation des données à l'ère de l'innovation numérique.

Conclusion

370. À travers ces observations, nous pouvons conclure que la mise en place des conditions générales de service répond à une double nécessité. D'une part, il existe une pression juridique, basée sur l'obligation de recueillir le consentement en amont, présente dans l'article 7 de la loi informatique et libertés[670]. De l'autre, il existe une nécessité économique et technique qui conditionne les services à recueillir celui-ci pour sécuriser leur principale source de revenus. Le recours à l'option « Do Not Track » comme refus exprès du suivi de l'internaute parait compromis au regard de l'objectif de valorisation des données. De même, les dispositions relatives la suppression du principe de recueil préalable à l'installation de cookies ciblés semblent hors propos, tant l'exploitation des données dépasse le cadre contraignant de leur utilisation limitée.

669 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

670 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 7.

371. Au final, cette conjonction des intérêts juridique et économique encourage le déploiement croissant des conditions générales de service sur l'ensemble des plateformes en ligne. Son étendue à l'ensemble des dispositifs de l'innovation technologique devient même l'un des enjeux du nouveau règlement Européen, qui sera applicable dès 2018[671] avec une nécessité de recueillir un consentement devenue bien plus formalisée. Ainsi : « *Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé* » [672]. En renforçant cette condition, le droit renforce la soumission de la protection de la vie privée au don du consentement.

372. Cette soumission va ensuite agir sur la capacité du service à valoriser les données. En recueillant un consentement étendu au traitement, celui-ci va pouvoir légitimer l'ensemble de ses opérations de valorisation. Or, dans la pratique, on peut observer que cette tendance légitime des collectes de plus en plus étendues des données personnelles. Dans cette configuration juridique, le service sera en mesure d'obtenir des données hétéroclites en provenance de l'utilisateur, sur lesquelles il aura obtenu une liberté presque totale de traitement.

373. Pour comprendre cela, il faut nous pencher sur l'étendue précise des collectes qui sont réalisées grâce à ce consentement aux conditions générales de service.

671 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, Article 99.

672 Ibid, considérant 32.

Section 2

Une collecte étendue légitimée par le consentement initial

374. Ainsi que le souligne Christiane Féral-Schul et Christian Paul, dans sa dimension juridique, « *le consentement est l'un des fondements de la protection des données à caractère personnel. Reconnue comme un droit fondamental en Europe, la protection des données personnelles est un élément de la liberté individuelle : sans une certaine maitrise de ce qui est divulgué à propos de soi, l'individu perd son autonomie par rapport aux autres. Le contrôle de chaque individu de ses données va donc au cœur de l'autodétermination informationnelle de l'individu* »[673]. Pourtant en pratique, d'autres avancent l'idée que celui-ci devient d'avantage un instrument de légitimation de la valorisation des données, plutôt que l'expression réelle de la volonté d'un individu, notamment au cœur des conditions générales de service.

375. Ainsi, pour Christophe Lazaro et Daniel Le Metayer : *« la majorité des personnes ne lisent pas ce type de document ou, lorsqu'ils les lisent, manquent des connaissances les plus élémentaires pour comprendre la portée et faire un choix informé en la matière. Dans le meilleur des cas, si les personnes lisent, comprennent et son susceptibles de faire un choix informé, les options qui leur sont offertes ne reflètent pas nécessairement leurs volontés* »[674]. Cela va créer un écart entre ce que la personne désir réellement, et les largesses qu'il va consentir au responsable de traitement pour valoriser les données.

376. Car dans les faits, le recours au consentement marque le début du traitement des données de l'utilisateur. Réalisée à l'initiative du responsable de traitement qui propose un service, cette valorisation est à mettre directement en rapport avec la capacité de collecte

673 Féral-Schul Christiane, Paul Christian, *Rapport d'information n°3119 sur le droit et les libertés à l'âge du numérique*, Déposé à l'Assemblée Nationale le 8 octobre 2015, p. 273.

674 Lazaro Christophe, Le Metayer Daniel, *Le Consentement au Traitement des Données Personnelles : une Perspective Comparative sur l'Autonomie du Sujet*, Revue juridique Thémis de l'Université de Montréal, voi.48 n°3, 2015, p 2.

initiale des données. Il y a donc un véritable enjeu pour le service à ce stade, qui a tout intérêt à y intégrer un maximum de données pour les exploiter par la suite.

377. Pour constater cet écart, nous verrons d'abord dans quelle mesure les conditions de licéité du traitement vont être interprétées de manière opportuniste dans la procédure de collecte (1). Ces dernières vont justifier la mise en place de collectes très étendues, d'abord des données de l'utilisateur (2), puis de celles qui sont accessibles à partir de ses terminaux (3). Nous pourrons observer que cette captation va même aller au-delà de la plateforme du service (4), pour toucher des sites tiers et suivre les pérégrinations de l'internaute à travers d'autres services. Grace à cela, le service va disposer d'un profil extrêmement précis de l'utilisateur, qu'il va être capable d'enrichir grâce à des procédés d'interconnexion de fichier avec des partenaires tiers (5).

1 – Une interprétation opportuniste des conditions de licéité du consentement dans la collecte des données

378. Pour les différents services mis à disposition des internautes dont le modèle économique est fondé sur le recueil et la vente de données à caractère personnel, les possibilités de valorisations dépendent de la capacité des algorithmes de traitements[675]. Une fois qu'une collecte a été réalisée, il s'agit de pouvoir compiler, organiser et croiser les données afin de les enrichir et construire un profil affiné de l'utilisateur, profil qui recèle une valeur supérieure pour les annonceurs cherchant à cibler un public déterminé. Par conséquent, le service qui dispose du logiciel le plus efficace pour réaliser ces taches dispose d'une capacité de valorisation supérieure face à ses concurrents.

379. Cependant, pour que l'algorithme soit efficace, il est nécessaire de l'alimenter à partir d'une base de données suffisante pour qu'il puisse créer ces profils ciblés, plus facilement exploitables pour les annonceurs. Ainsi, « *l'utilisation de technologies reposant sur des*

675 Certains chercheurs mettent en avant leur impact, et demandent une ouverture de ces algorithmes aux autorités pour pouvoir juger des traitements effectifs. v. Mayer-Schonberger Viktor, Cukier Kenneth, *Big Data : A Revolution that Will Transform How We Live, Work and Think*, Eamon Dolan and Houghting Mifflin Harcourt, 5 mars 2013, 256 p. Ainsi que : Conseil National du Numérique, *Rapport Ambition Numérique : Pour une politique Française et Européenne de la transition numérique*, Rapport remis au Premier Ministre, Juin 2015, p. 77.

algorithmes prédictifs nécessite une exploitation de données, en vue d'effectuer des calculs statistiques et probabilistes permettant de prédire un comportement, d'émettre un diagnostic, d'anticiper une situation, etc. Or, seuls un recueil et une exploitation massive de données peuvent permettre d'obtenir des résultats concluants » [676]. Par conséquent, l'opération de collecte de données, qu'elle soit réalisée à travers le site web, ou bien par l'acquisition de base de données en provenance de site tiers, devient un enjeu financier équivalent à celui de l'amélioration des techniques algorithmiques.

380. D'un point de vue juridique, ces deux actions, collecte puis analyse algorithmique, que l'on peut distinguer sur un plan pratique, sont soumises à un unique régime: celui applicable aux traitements de données à caractère personnel issu de la loi du 6 janvier 1978 modifiée[677]. Peu importe sur quelle phase agit précisément l'algorithme, il y sera soumis dès l'intégration des premières données.

381. Comme précédemment exposé, une grande partie de la licéité repose sur le consentement de l'utilisateur. Or, dans la plupart des cas, on peut reprocher aux conditions générales d'être très exigeantes en matière d'autorisations de collectes et de traitements de données. À titre d'exemple, nous pouvons nous pencher sur la récente notification de mise en demeure de la CNIL à l'égard de Facebook sur la mise en conformité de ses pratiques vis-à-vis de la loi informatique et libertés[678]. Celle-ci présente un double intérêt. D'une part, elle s'appuie principalement sur le manque d'informations données aux utilisateurs sur le périmètre et le traitement exact des données, fondement du consentement. D'autre part, elle met en lumière une captation des données très étendue de la part d'un service incontournable sur internet.

382. En l'espèce, le réseau social capte l'ensemble des données que l'utilisateur va donner lors de son inscription. Ce faisant, il collecte des données hétérogènes lors de l'utilisation du

676 Bensoussan Alain, *Algorithmes Prédictifs et Protection des Données Personnelles*, Alain Bensoussan Avocats, 19 novembre 2015, disponible sur https://www.alain-bensoussan.com/algorithmes-predictifs-2/2015/11/19/ (consulté le 01/09/17).

677 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés,* modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 7.

678 Commission Nationale de l'Informatique et des Libertés, *La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi informatique et libertés*, Communication datée du 9 février 2016, disponible sur https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi (consulté le 01/09/2017).

service à travers le temps. Ainsi, d'après sa politique d'utilisation des données[679], Facebook procède à un recueil des informations fournies par l'utilisateur, « *notamment lorsque vous* [l'utilisateur] *créez un compte, créez ou partagez du contenu ou encore lorsque vous communiquez avec d'autres personnes. Ceci peut comprendre des informations concernant le contenu que vous partagez, telles que le lieu d'une photo ou encore la date à laquelle un fichier a été créé. Nous recueillons également des informations concernant la manière dont vous utilisez nos Services, telles que les types de contenu que vous consultez ou avec lesquels vous interagissez, ou encore la fréquence et la durée de vos activités* » [680].

383. Dans les faits, ces indications couvrent la totalité des données qui peuvent être extraites de la relation que l'utilisateur va entretenir avec le service, depuis son départ jusqu'à sa conclusion, sans tenir compte de leurs particularités relatives. Ainsi, bien que cela ne soit pas clairement indiqué lors de l'examen de la Politique d'utilisation des données, on peut trouver une référence directe dans les règles publicitaires[681] à la race, l'origine ethnique, la religion, les croyances, l'orientation sexuelle, l'identité sexuelle, le handicap, l'état de santé, la situation financière, l'appartenance à un syndicat, ou des informations sur le casier judiciaire d'une personne. Si l'on cherche à effectuer une campagne publicitaire à partir de ses services, on se rend compte qu'il est possible d'utiliser de telles données lors de la création d'une campagne ciblée, par exemple pour classer les personnes selon leurs « *affinités ethniques* » ou si ceux-ci sont intéressés par des hommes ou des femmes[682].

384. Or, si les informations disponibles sur le profil Facebook d'une personne relèvent du régime applicable aux données à caractère personnel, les éléments précités constituent des données sensibles au sens de l'article 8-I de la loi informatique et libertés qui dispose : «*Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont*

679 Facebook, Politique d'utilisation des données, version datée du 30 janvier 2015, disponible sur https://fr-fr.facebook.com/about/privacy (01/09/2017).

680 Ibid.

681 Facebook, Règles publicitaires, version datée du 5 mai 2016, disponible sur https://www.facebook.com/policies/ads/#overview (01/09/2017).

682 Facebook, Outil de gestion de création de campagne publicitaire, disponible sur https://www.facebook.com/ads/manager/creation/ (Consulté le 01/09/2017).

relatives à la santé ou à la vie sexuelle de celles-ci » [683]. En application de l'article 8-II-1[684], Il sera nécessaire que le service recueille le consentement des utilisateurs pour effectuer un tel traitement, et a fortiori, pour les vendre à travers son service de publicités ciblées.

385. Cette étape cruciale dans l'information et le recueil du consentement est quasiment absente puisque, lors de l'inscription au service, seul un bouton « *inscription* » [685] est présent sur la page. Une mention relative aux conditions du service, aux politiques d'utilisation des données et aux règles d'utilisation des cookies est indiquée, mais son acceptation n'est pas distincte de l'inscription au service, et ne nécessite aucun « *clic* » supplémentaire.

386. À la lumière de ces observations, la CNIL va considérer que ce recueil de données sensibles est fait sans *« le consentement exprès des internautes lors de la collecte et du traitement des données relatives à leurs opinions politiques, ou religieuses, et à leur orientation sexuelle. De même, aucune information n'est délivrée aux internautes sur leurs droits et sur l'utilisation qui sera faite de leurs données sur le formulaire d'inscription au service* » [686]. Dans cet argumentaire, le consentement et l'information suffisante de l'utilisateur apparaissent comme les gardiens nécessaires de la licéité de la collecte des données.

387. Mais en analysant les dispositifs publicitaires offerts par le réseau social aux annonceurs, on constate un écart important entre la précision des informations fournies aux utilisateurs dans les conditions générales de service sur les données traitées et les possibilités offertes par les campagnes dites « *de publicité ciblée* ». Dans le premier cas, on utilise des

683 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 8.

684 « *Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 1 – les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut pas être levée par le consentement de la personne concernée* ». Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 8-II-1.

685 v. Page d'inscription à Facebook, disponible sur https://fr-fr.facebook.com/r.php (consulté le 01/09/17).

686 Commission Nationale de l'Informatique et des Libertés, *La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi informatique et libertés*, Communication datée du 9 février 2016, disponible sur https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi (consulté le 01/09/2017).

termes génériques, de l'autre, une précision monnayable dans le ciblage d'informations sur les utilisateurs[687].

388. Dès lors, l'argumentaire de la CNIL valant pour les données sensibles peut être étendu de manière plus large aux données fournies par l'utilisateur dans son ensemble. Si pour une catégorie de données, le consentement n'est pas licite pour défaut d'information, est-il possible que ce consentement unique subsiste malgré sa révocation partielle ? En somme, le consentement est-il considéré comme un bloc unique facteur de licéité, ou bien peut-il être décomposé ?

389. Ce questionnement devient un enjeu central dans ces nouveaux traitements issus de l'innovation numérique, qui sont par essence étendus, et dont les finalités évoluent en fonction des techniques algorithmiques. Or, la révocation de la licéité d'une partie des données traitées entrainerait une insécurité juridique réelle pour les services. L'intérêt pour les services sera alors de faire une interprétation opportuniste des conditions de licéité du consentement, en concentrant l'ensemble de leurs différentes politiques de confidentialité dans un même document, à l'instar des modifications récentes effectuées par Google. L'ensemble des traitements et des données seront donc détaillés sur un même support, sans distinction. Dès lors, si l'utilisateur souhaite ne s'inscrire qu'à un seul service, les données exploitées par l'ensemble des services de Google seront collectées. Ainsi comme nous allons pouvoir l'observer, en tentant de reformer une exigence de formalisme, le règlement Européen va conduire à une exploitation bien plus étendue des données.

2 – La possibilité d'une collecte maximale des données par le recours systématique au consentement

390. En supposant que les règles de confidentialité soient d'un formalisme rigoureux, celles-ci détaillent de façon exhaustives les traitements dont feront l'objet les données à caractère personnel pour répondre aux différentes règles de droit que nous avons évoqué précédemment. Ainsi, à l'instant où le consentement est recueilli, l'internaute donne son

687 Facebook, outil de gestion de création de campagne publicitaire, disponible sur https://www.facebook.com/ads/manager/creation/ (Consulté le 01/09/2017).

accord à l'ensemble des traitements et finalités exprimées. Dans les faits, il s'agira pour le service de construire un profil précis de l'utilisateur en ce qui concerne ses gouts, ses habitudes, ses fréquentations et ses tendances d'achats pour que la valeur du profil soit supérieure à l'achat pour une régie publicitaire. Dans cette optique, de nouveaux équipements cherchent à capter jusqu'aux émotions de l'utilisateur[688], la direction du regard et l'ordre de lecture des différentes informations affichées[689].

391. Mais au-delà de cet objectif primaire de valorisation, il existe un objectif secondaire visant à consolider la place du service dans le paysage numérique. Pour cela, les services cherchent des moyens d'améliorer l'expérience utilisateur. Dans un souci d'optimisation et de fidélisation, ils doivent innover et s'adapter à l'utilisation pratique de leur service par les internautes. Un second ensemble de données hétérogènes est alors ciblé, telles que la rapidité de navigation, le temps d'affichage, les frappes du clavier, les mouvements de souris, etc.

392. Dans ce cadre, la rédaction des règles de confidentialité constitue une opportunité à saisir pour le service afin de légitimer l'utilisation d'un maximum de données. En décrivant l'ensemble des données qu'il collecte, il se donne la possibilité de les traiter avec l'accord de l'utilisateur. Un exemple particulièrement intéressant est observable à travers les règles de confidentialité de Google, notamment après la sanction de la CNIL en 2014 qui a conduit à une refonte profonde des règles de confidentialité applicable au service[690].

393. Aujourd'hui, les règles de confidentialité de Google détaillent sur 11 pages l'utilisation des données qui est faite sur ses services[691]. On peut également y trouver une mention relative à des conditions d'utilisations[692] précisant d'autres types de traitements dans un souci d'exhaustivité. Celles-ci sont accessibles directement sur le site internet à travers un lien présent en bas de chaque page des services de Google. Le consentement à ces conditions est obligatoire pour accéder aux services lors de l'enregistrement du compte. Cela consiste en

688 Mao Qi-rong, Pan Xin-yu, Zhan Yong-zhao, Shen Xian-jun, *Using Kinect for real-time emotion recognition via facial expressions*, Frontiers of Information Technology & Engineering, 2015 16(6), pp. 272-282.

689 Girard Laurence, *Le retour des écrans publicitaires dans le métro*, Le Monde, 29 avril 2010.

690 Commission Nationale de l'Informatique et des Libertés, *Délibération n°2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc*.

691 Site internet de Google, disponible sur https://www.google.fr/intl/fr/policies/privacy/ (consulté le 01/09/2017).

692 Site internet de Google, disponible sur https://www.google.fr/intl/fr/policies/terms/regional.html (consulté le 01/09/2017).

l'affichage d'un résumé des conditions d'utilisation et de confidentialité des services, sur lequel l'internaute peut obtenir les versions complètes des deux textes. Un bandeau d'information relatif aux cookies a été ajouté, de manière à être présenté à l'internaute lors de la première visite. L'utilisateur peut alors, de manière classique, obtenir des informations supplémentaires sur la politique d'utilisation des données, et continuer la navigation sur le site pour manifester son accord avec celles-ci.

394. L'un des éléments reprochés par la décision était le manque de clarté des règles de confidentialité sur les données recueilles[693]. Dans sa version datée du 28 juin 2016, Google indique que les données collectées seront : « *les informations que vous nous communiquez […] telles que votre nom, adresse email, numéro de téléphone ou carte de paiement* » [694]. Mais également les informations que Google collecte lors de l'utilisation des services « *lorsque vous regardez une vidéo sur Youtube, lorsque vous vous rendez sur un site web sur lequel nos service publicitaires sont utilisés ou lorsque vous consultez nos contenus et nos annonces, et que vous effectuez des actions sur celles-ci* » [695]. Ainsi, seront collectées : les données relatives à l'appareil utilisé, les fichiers journaux, les données de localisation, le numéro d'application unique et les cookies. Il est précisé que les informations personnelles recueillies sont susceptibles d'être recoupées avec celles « *d'autres services Google* » [696]. En ce qui concerne les contenus, cela peut être « *des informations variées : préférences et données liées à votre utilisation des services, messages Gmail, profil G+, photo, vidéos, historique de navigation, recherches sur des cartes, documents ou tout autre contenu hébergé par Google* » [697]. Il s'agit ici d'une quantité colossale de données.

395. En s'autorisant à traiter des informations issues des conversations, des emails, ou des documents numériques placés sur le service cloud Gdrive[698], Google s'offre une manne de données considérable en l'échange du consentement de l'utilisateur. Les informations présentes dans les photos, ou les vidéos personnelles de l'utilisateur sont alors soumises aux

693 Commission Nationale de l'Informatique et des Libertés, *Délibération n°2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc*.
694 Règles de confidentialité de Google, disponible sur https://www.google.fr/intl/fr/policies/privacy/, (consulté le 01/09/2017) p1.
695 Ibid. p1.
696 Ibid. p7.
697 Ibid. p7.
698 Service de stockage de documents en ligne Google Drive, disponible sur https://www.google.com/intl/fr_fr/drive/ (consulté le 01/09/2017).

algorithmes variés de Google afin d'en extraire un maximum de données valorisables, et cela, quel que soit le service auquel l'utilisateur souhaitait accéder à l'origine.

396. Cette action pourrait être interprétée comme une extension des prérogatives du responsable de traitement dans le cadre du régime protecteur des données à caractère personnel. En s'attachant à qualifier la chronologie du traitement, on peut douter du fait qu'une vidéo ou une photo placée sur le service de Google soit une donnée à caractère personnel en l'état. L'exemple le plus frappant étant celui de l'analyse des messages de l'utilisateur qui dépend du régime des correspondances privées[699] puisqu'il s'agit d'un « *message exclusivement destiné à une ou plusieurs personnes, physique ou morales, déterminées et individualisées* » [700]. L'article 226-15 du Code Pénal vient d'ailleurs sanctionner toute ouverture ou détournement des correspondances de mauvaise foi.

397. Mais grâce à leur rédaction et à leur unicité, Google va s'appuyer sur le consentement à ses conditions de services et à ses règles de confidentialité pour contourner les limites imposées par le code pénal, et traiter des données qui ne sont pas des données à caractère personnel à l'origine. De plus, si juridiquement le consentement légitime le traitement des données, sa licéité dépend en grande partie de l'étendue et de la précision avec laquelle celles-ci sont définies dans les conditions générales de service. En pratique, on peut observer, à travers les exemples successifs des conditions générales de Facebook et Google, une tendance à une certaine opacité dans la définition des algorithmes et des données recueillies. Or, c'est dans cet espace « *gris* » que la plupart des collectes et des traitements se placent.

398. Cette observation donne lieu à interrogation. D'un côté, le consentement est le pilier de la licéité des traitements. De l'autre, on peut constater qu'en pratique il donne aux responsables de traitement un accès quasiment illimité aux données que l'utilisateur va livrer pendant son utilisation du service. Cet accès s'accompagne d'une grande liberté donnée à la définition des algorithmes qui seront déployés, pouvant aller jusqu'à l'extraction de données personnelles à partir de matériel brut, comme les photos ou les vidéos. Enfin, on peut constater que cette extraction ne se limite pas seulement aux données de l'utilisateur.

699 Régime qui est appliqué aux correspondances électroniques puisque le terme « *correspondance désigne toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts* ». TGI. Paris, 17eme chambre, Chambre de la presse, Jugement du 2 novembre 2000.
700 TI. Puteaux, 28 septembre 1999.

3 – Une collecte des données possible grâce à l'accès au terminal de l'utilisateur

399. À celles-ci, s'ajoute l'extraction des données que l'utilisateur peut fournir indirectement. Dans la politique d'utilisation des données de Google, on peut remarquer la mention d'une fonction de captation des « *données d'emplacement de l'appareil, notamment les données d'emplacement géographique précises recueillies à travers les signaux GPS, Bluetooth ou Wi-Fi* »[701]. Ces informations, prises dans leurs ensembles, permettent de localiser avec précision un utilisateur, tout en transformant son terminal en capteur de données vis-à-vis des signaux Bluetooth ou Wi-Fi qui seraient à proximité.

400. Ces signaux sont en général émis par des boitiers d'accès à internet fournis par les opérateurs de réseaux à leurs abonnés[702]. Ils peuvent directement faire apparaitre le nom de la personne et, associés à une adresse MAC fixe, ils constituent un moyen simple d'identification du signal[703]. Lorsque l'utilisateur active le Global Positioning System (GPS) de son terminal, l'application associera les coordonnées GPS avec les signaux Wi-Fi perçus, et réalise une cartographie de leurs présences. Lors de l'absence de signal GPS, le service pourra déterminer la position de l'utilisateur à partir des réseaux Wi-Fi à proximité préalablement localisés.

401. Ce type de captations a déjà été visé par la CNIL. Dans sa délibération n°2011-035[704], la Commission prononçait une sanction pécuniaire à l'encontre de la société Google pour avoir réalisé une telle collecte lors du passage de ses « *Google Car* » dans les rues Françaises. En l'espèce, le service de cartographie se servait de véhicules équipés spécialement pour réaliser des photographies des rues traversées pour son développer son service « *Google*

701 Règles de confidentialité de Google, disponible sur https://www.google.fr/intl/fr/policies/privacy/, (consulté le 01/09/2017) p1.

702 A titre d'exemple, on peut trouver cette option sur la plupart des « box » fournies par les opérateurs internet.

703 Une adresse MAC est l'identifiant physique de la carte réseau du terminal, différente de l'adresse IP ou du SSID réseau qui peuvent être changés facilement par l'utilisateur. Pour plus d'informations, v. Cozette Philippe, *Programmer pour Internet : Notions fondamentales et Mise en Pratique*, Editions ENI, 6 février 2007, 633 p.

704 Commission Nationale de l'Informatique et des Libertés, *Délibération n°2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc*. Disponible sur https://www.cnil.fr/sites/default/files/typo/document/D2011-035.pdf (Consulté le 01/09/2017).

Street View ». Lors de ses passages, le véhicule relevait également des informations « *sur les adresses MAC et les identifiants SSID des points d'accès Wi-Fi se trouvant à proximité de ceux-ci […]. Elle* [L'analyse de la CNIL] *a par ailleurs permis d'établir que les « Google cars » enregistraient non seulement les adresses MAC des points d'accès Wi-Fi, mais aussi les adresses MAC de l'ensemble des terminaux connectés à ces points d'accès (ordinateurs personnels, imprimantes et autres périphériques, Smartphones, etc.)* » [705].

402. S'il existait un doute sur l'applicabilité du régime des données personnelles à ce type d'informations, la CNIL précisera que ces données « *doivent être considérées comme des données à caractère personnel au sens de la loi* » [706], confirmant son analyse exprimée pour la première fois dans sa communication du 2 Août 2007[707]. Pour se justifier, la Commission s'appuie sur le fait « *qu'une adresse MAC, qui n'identifie que le routeur Wi-Fi qui permet aux utilisateurs d'accéder à internet, ne peut être qualifiée, à elle seule, de données à caractère personnel. En revanche, une adresse MAC peut être captée par des sites internet lors de la navigation de l'Internaute, après que ce dernier se soit identifié. Une fois reliée à ces éléments d'identification, elle constitue nécessairement une donnée personnelle. C'est en fonction de tels éléments de contexte qu'il convient de décider si une adresse MAC peut être considérée, ou non, comme une donnée à caractère personnel* » [708].

403. En l'espèce, les Google Cars ont effectué des relevés GPS permettant de localiser ces signaux. Ainsi, « *la finalité de la collecte des adresses MAC, combinées aux autres informations collectées, conduit la formation restreinte à considérer que ces données, combinées entre elles, constituent des données à caractère personnel* » [709]. Cet argumentaire est d'ailleurs renforcé : lors de l'analyse de ces données, la CNIL a constaté la captation d'informations supplémentaires sur certaines personnes qui n'avaient pas suffisamment sécurisé leurs émetteurs Wi-Fi, en enregistrant les sites visités ainsi que les comptes et mots de passes associés[710].

705 Ibid. p3-p20.
706 Ibid. p26.
707 Commission Nationale de l'Informatique et des Libertés, *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL Européennes*, 2 Août 2007.
708 Ibid. p20.
709 Ibid. p20.
710 La CNIL a constaté que les informations données ont permis de parvenir à un certain nombre de rapprochements permettant d'identifier des personnes. Ainsi « - *le 2 juin 2008, à 12h46, un internaute situé selon les données GPS à proximité d'une adresse très précise, dans la ville de MARSEILLE (13007), accède*

404. D'un point de vue technique, ces captations ne nécessitent pas le consentement du propriétaire du routeur Wi-Fi et rendent difficilement applicable l'obligation d'information individuelle puisqu'elles s'effectuent à distance. Dans ses réponses apportées à la CNIL lors de la procédure, Google avait mis en avant l'article 32-III de la loi Informatique et libertés[711] qui dispose : « *Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées au I dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données […] Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche* ».

405. L'argument fut balayé par la Commission restreinte qui, bien qu'admettant « *que l'information individuelle des titulaires des adresses MAC et des identifiants Wi-Fi est effectivement impossible à mettre en œuvre dans de telles circonstances* » [712], estimera que « *la société ne saurait s'exonérer d'une information générale sur la collecte de ces données et sur les droits des personnes à cet égard* » [713]. Dès lors, considérant que le service n'a mis en place aucune procédure pour informer les personnes de ces captations, la formation restreinte va retenir « *le caractère déloyal de la collecte des données* » et prononcer une sanction pécuniaire de 100 000€[714] à son encontre.

406. En corollaire, on peut supposer que toute collecte d'informations telles que les signaux Bluetooth et Wi-Fi réalisée grâce au terminal de l'utilisateur sera déloyale dans les mêmes

---

à un site d'image pornographiques appelé http://www.straightboysjerkoff.com, dont il est membre. L'identifiant qu'il utilise sur le site est enregistré en clair [Dans la base de données de la Google Car], ainsi que son mot de passe et son adresse IP sur le réseau internet, connecté à son point d'accès. L'identifiant SSID et l'adresse MAC de son point d'accès sont connus de Google mais ont été supprimés des informations fournies à la CNIL ». Commission Nationale de l'Informatique et des Libertés, *Délibération n°2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc*. p10, Disponible sur https://www.cnil.fr/sites/default/files/typo/document/D2011-035.pdf (Consulté le 15/06/16).

711 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004.

712 Commission Nationale de l'Informatique et des Libertés, *Délibération n°2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc*. disponible sur https://www.cnil.fr/sites/default/files/typo/document/D2011-035.pdf (Consulté le 01/09/2017).

713 Ibid.

714 Ibid.

conditions. La transmission de ces données sera considérée comme illicite, d'autant que ni la destination exacte de ces données, ni la nature complète de la collecte n'est définie en amont. Toutefois, cette analyse de vaut que si l'on se place au niveau de la responsabilité du service. En considérant que l'utilisateur est suffisamment avertit de la collecte, et que celui-ci dispose d'une certaine maitrise sur l'accès de l'application aux réseaux à proximité, est-il possible de caractériser un transfert de la responsabilité ? Ce qui est certain, c'est que l'accès à ces données est autorisé par le consentement aux conditions générales.

4 – Une acquisition des données étendue au dehors du périmètre dédié au service

407. Bien que les collectes précédemment évoquées soient particulièrement larges, nous devons également prendre en compte les informations provenant de partenaires tiers. À titre d'exemple, nous pouvons lire dans les conditions de Facebook : « *Nous recevons des informations sur vous et vos activités, sur et en dehors de Facebook, en provenance de nos partenaires tiers, telles que des informations provenant de partenaires avec qui nous avons collaboré pour offrir un service, ou encore d'annonceurs au sujet de votre expérience ou de votre interaction avec ce dernier* » [715].

408. Ce type de collectes peut être réalisé par le biais de deux technologies différentes[716]. La première, grâce à la mise en place sur des sites partenaires de plugins sociaux, nouveau outils d'un colonialisme numérique. La seconde, en faisant appel aux procédés classiques d'interconnexion et d'achat de base de données, dont les possibilités son décuplées par les nouveaux outils algorithmiques, que nous verrons dans le point suivant.

409. Concernant la première méthode, celle-ci découle directement de l'ingéniosité et de l'essor des sites et médias sociaux. Création idoine, le plugin social s'appuie sur un réseau social fort de sa base utilisateur, et offre un service de visibilité supplémentaire à un site internet en échange de sa présence sur ces pages. Ce sont « *des applications liées aux*

715 Facebook, Politique d'utilisation des données, version datée du 30 janvier 2015, disponible sur https://fr-fr.facebook.com/about/privacy (consulté le 01/09/2017).
716 v. Loukouman Amidou, *Marketing des Réseaux Sociaux*, MA Editions, 22 février 2012, 264 p.

différents médias ou réseaux sociaux (Facebook, Twitter, Youtube, Viadeo, etc..) qui peuvent être placées sur un site tiers par un simple copier / coller de code fourni par la plateforme sociale. Pour le site d'accueil, les plugins sociaux peuvent permettre notamment de proposer la recommandation de contenus, d'utiliser des données de profils pour des commentaires, l'enregistrement ou la complétion de formulaires ou d'afficher des contenus en provenance des sites sociaux »[717]. Le bouton « *like* » que nous voyons sur différents sites en est l'exemple type.

410. Pour le site internet partenaire, cela permet de donner une grande facilité à ses membres pour partager son contenu sur les réseaux sociaux, et ainsi générer un trafic supérieur sur son propre site. Pour le réseau social, cela permet de recueillir de nouvelles informations sur la personne à partir du site visité. Ainsi : « *si une personne a visité Facebook et votre site partenaire ayant un plugin social, le navigateur nous informe afin que Facebook puisse afficher son contenu sur cette page. Les données que nous pouvons recevoir incluent l'identification numérique de la personne, le site internet visité, la date et l'heure ainsi que d'autres informations liées au navigateur. Nous enregistrons ces informations et pouvons les utiliser pour améliorer nos produits et service, ainsi que pour montrer aux personnes des publicités plus intéressantes et utiles* »[718].

411. Cette pratique permet d'accroitre le périmètre de captation des données tout en enregistrant des informations sur les sites visités par l'utilisateur. Or, il est apparu à la CNIL que cette collecte visait également les personnes qui ne disposaient pas de compte Facebook. Dans sa décision datée du 9 février 2016, « *La CNIL a constaté que le site FACEBOOK est en mesure de suivre la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte FACEBOOK. En effet, le site dépose un cookie sur le terminal de chaque internaute qui visite une page FACEBOOK publique, sans l'en informer*

717 Bathelot Bertrand, *Définition: Plugins sociaux*, Définitions Marketings, Encyclopédie illustrée du marketing, 28 juillet 2015, disponible sur http://www.definitions-marketing.com/definition/plugins-sociaux/ (consulté le 01/09/2017).

718 Traduction par l'auteur de: « *If a person has visited Facebook and visits your website* [Le site partenaire] *with a social plugin, the browser sends us information in order to load Facebook content on that page. The data we receive may include info like the person's user ID, the website they're visiting, the date and time, and other browser-related info. We record some of this info and may use it to improve our products and services and to show people more interesting and useful ads* ». Facebook for Developers, Social Plugins FAQs, General Questions, What information does Facebook get when I implement a social plugin, and how is it used, disponible sur https://developers.facebook.com/docs/plugins/faqs/#faq_574746276036649 (consulté le 01/09/2017)

(pages d'un événement public ou d'un ami par exemple). Ce cookie permet alors au site d'identifier tous les sites internet sur lesquels cet internaute se rend dès lors qu'ils contiennent un bouton FACEBOOK (« J'aime » ou « Se connecter » par exemple) »[719]. Le réseau est capable de suivre un internaute dans sa navigation sur une grande partie du réseau internet. Dès 2010, plus de 50 000 sites internet disposaient de tels boutons[720].

412. La mise en place d'un tel plugin ne saurait être neutre d'un point de vue juridique. A travers l'intégration de cette technologie, le site internet devient un préposé à la collecte des informations pour le réseau social. La question sa responsabilité peut être posée pour savoir si celui-ci prend une part active dans la collecte des données à caractère personnel, et par conséquent, s'il devient responsable de celle-ci conjointement avec le réseau social.

413. Pour déterminer ce niveau de responsabilité, il faut d'abord rappeler que le consentement de l'utilisateur est un élément primordial dans la licéité du traitement et que celui-ci est évalué à l'instant de la première collecte. Le responsable sera celui qui déterminera les finalités de ce traitement[721]. En apposant sur son site internet un plugin social, le directeur de la publication participe-t-il à la détermination de ces finalités ? Pour y répondre, il faut comprendre le fonctionnement interne du plugin social, à l'instar de la décision du 9 mars 2016 du tribunal régional de Düsseldorf[722].

414. En l'espèce, il s'agit d'un litige opposant un site internet et une association de consommateurs sur la responsabilité dans la mise en place de tels plugins. Pour y répondre, le tribunal va en premier lieu procéder à des analyses techniques des codes sources des plugins,

719 Commission Nationale de l'Informatique et des Libertés, *La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi informatique et libertés*, Communication datée du 9 février 2016, disponible sur https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi (consulté le 01/09/2017).

720 Nick O'Neill, *50 000 websites add Facebook's Like button and social plugins in first week*, Adweek, 28 April 2010, disponible sur http://www.adweek.com/digital/50000-websites-add-facebooks-like-button-and-social-plugins-in-first-week/ (consulté le 01/09/17).

721 *«responsable du traitement»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire* ». Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel n° L281 du 23/11/1995 p.0031-0050, Article 2.

722 LG Düsseldorf, Urteil vom 09/03/2016, Az.: 12 O 151/15.

ainsi que de la façon dont les données sont collectés, transmises et stockées. Celles-ci vont confirmer que le plugin social de Facebook recueille les adresses IP des internautes sur le site où il est placé.

415. La transmission de ces informations est faite directement du terminal de l'utilisateur vers les serveurs de Facebook, sans que le serveur du site internet ait une quelconque action technique à réaliser. Ces données ne lui sont donc pas transmises. Cependant, le tribunal estimera que la mise en place de ce plugin révèle une démarche positive de la part du site internet. Par conséquent, il acquiert la responsabilité du traitement par son rôle actif dans la mise en place de la collecte. Le fait de n'avoir pas suffisamment informé les internautes entrainera la nullité de leur consentement général à la collecte de donnée, et le tribunal condamnera le site web.

416. De cette décision on peut déduire deux choses. D'une part, que la mise en place d'un plugin social engendre une responsabilité vis-à-vis de la collecte de données réalisée. D'autre part, que la présence d'une page d'information exhaustive et une procédure de recueil du consentement doivent être mises en place pour que celles-ci soient licites. Or, il existe une nouvelle fois une disparité dans l'information donnée à l'utilisateur. Si la collecte est effectuée par un service tiers disposant d'un plugin social, l'information sur la finalité du traitement ne peut être que dépendante de l'information disponible à l'origine dans les conditions d'utilisation du service. Or, nous avons vu que celles-ci sont le plus souvent parcellaires. De plus, le responsable de la publication devient responsable d'une collecte dont il ne peut maitriser l'étendue. Cet état contribue à fragiliser la valeur du consentement de l'utilisateur dont on peut douter du recueil légitime dans l'ensemble des 10 millions de sites internet sur lesquels ces plugins sont présents[723].

723 Zephoria, *Top 20 valuable Facebook Statistics,* Juillet 2016, disponible sur https://zephoria.com/top-15-valuable-facebook-statistics/ (consulté le 01/09/2017).

5 – Une acquisition des données par interconnexion

417. Il existe une seconde pratique qui a pour objectif d'étendre le périmètre de la collecte de données. Celle-ci utilise des techniques classiques d'acquisitions ou d'interconnexions de bases de données sur fond contractuel, mais bénéficie des nouvelles possibilités offertes par les algorithmes de traitement. Ainsi, à travers une politique de partenariats efficace, différentes entités peuvent trouver un intérêt commun à partager leurs données et les informations qu'ils détiennent sur leurs utilisateurs. C'est le cas notamment de la grande distribution, qui se dote d'outils de pointe pour gérer ces bases de données comprenant parfois jusqu'à 13.7 millions de personnes[724]. Ceux-ci sont en mesure d'offrir à leurs clients professionnels un moyen d'avoir une visibilité sur les ventes réalisées, en pouvant identifier les acheteurs individuellement.

418. De même, un service disposant d'information géographique sur ses utilisateurs peut lier l'affichage d'une publicité à une visite en magasin. En ajoutant à cela l'article acheté, on obtient un profil utilisateur qui possède une valeur bien supérieur pour un annonceur potentiel. C'est dans cette direction que les principaux services internet se sont lancés ces dernières années. Google a lancé « *Store Visits* » en Janvier 2015, service proposant aux annonceurs de les prévenir lorsqu'un utilisateur ayant vu une publicité spécifique se rend dans leur magasin[725]. Facebook répliqua avec « *In Store* », service similaire en Juin 2016[726].

419. Pour que ces services génèrent un profil utilisateur ayant une valeur supérieure, il faut nécessairement une forme d'interconnexion entre les données du réseau social et celles du distributeur. Or, l'interconnexion est susceptible d'une déclaration, voire d'une autorisation préalable de la part de la CNIL en fonction de certains éléments. Soumis au régime des articles 23, 25 et 27 de la loi Informatique et libertés[727], l'autorité nationale a précisé les éléments permettant de définir le régime applicable.

---

724 Clapaud Alain, *ROI, Croisement des données, volatilité des clients : Carrefour monétise ses Datas*, La revue du Digital, disponible sur http://www.larevuedudigital.com/roi-croisement-des-donnees-volatilite-des-clients-big-data-tout-sur-la-strategie-de-carrefour-medias/ (consulté le 01/09/2017).

725 Voir site web de Google Adwords Help, About store visit conversions, disponible sur https://support.google.com/adwords/answer/6100636?hl=en (Consulté le 01/09/2017).

726 Voir site web de Facebook Buisiness Help, disponible sur https://www.facebook.com/business/news/drive-and-measure-store-visits-and-sales (Consulté le 01/09/2017).

727 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de*

420. Le premier critère concerne l'objet de l'interconnexion, qui doit être la « *mise en relation de fichiers ou de traitements de données à caractère personnel* » [728]. Caractérisée par « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* » [729], on peut supposer que cette condition est remplie par la plupart des traitements relatifs aux données des utilisateurs de réseaux sociaux, de même qu'aux éventuels clients des distributeurs.

421. Le second critère nécessite la mise en relation d'aux moins deux fichiers ou traitements distincts. La CNIL précise que « *l'ajout d'informations dans un fichier existant ou la modification des finalités d'un traitement ne constituent pas à eux seuls des formes d'interconnexion, quand bien même ces ajouts nécessitent des moyens techniques nouveaux* »[730]. Cependant, il est important de noter que « *la notion d'interconnexion peut s'appliquer aux fichiers d'un même responsable de traitement* »[731].

422. Le troisième critère s'applique lorsqu'il « *s'agit d'un processus automatisé ayant pour objet de mettre en relation des informations issues de ces fichiers ou de ces traitements* »[732]. L'interconnexion peut alors prendre différentes formes : « *Elle peut être à sens unique : un fichier peut servir à enrichir les informations contenues dans un deuxième fichier. On parle alors « d'alimentation ». Elle peut être bidirectionnelle : des échanges peuvent s'effectuer dans les deux sens, lorsque des informations issues d'un traitement sont envoyées vers un deuxième traitement, pour obtenir en retour une information nouvelle ou sa confirmation. On parle généralement de « fichier d'appel » et de « fichier réponse » pour décrire ces échanges. Elle peut aboutir à la création de nouveaux flux : Des fichiers issus de deux traitements*

---

données à caractère personnel, Publiée au Journal Officiel du 7 août 2004.

728 Commission Nationale de l'Informatique et des Libertés, *Notion d'interconnexion*, Communication datée du 5 avril 2011, disponible sur https://www.cnil.fr/fr/comment-determiner-la-notion-dinterconnexion (Consulté le 01/09/2017).

729 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 2.

730 Commission Nationale de l'Informatique et des Libertés, *Notion d'interconnexion*, Communication datée du 5 avril 2011, disponible sur https://www.cnil.fr/fr/comment-determiner-la-notion-dinterconnexion (Consulté le 01/09/2017).

731 Ibid.

732 Ibid.

distincts peuvent être rapprochés ou comparés pour obtenir une information nouvelle ou la consolidation d'informations existantes. Elle peut être ponctuelle : Une interconnexion peut être effectuée de manière automatisée mais ponctuelle, pour un besoin particulier : une fois lors de la création du traitement, ou de manière périodique (par exemple 1 fois par mois). Elle peut être permanente : L'interconnexion peut nécessiter la mise en œuvre de moyens de communication permanents entre les différents fichiers qui la composent, par exemple pour réaliser des traitements en temps réel »[733].

423. Pour ces catégories d'interconnexions, une simple déclaration à la CNIL sera nécessaire. Mais il existe un quatrième critère qui limite l'interconnexion de fichiers à l'obtention d'une autorisation préalable. Si les « *fichier interconnectés sont issus de traitements ayant des finalités différentes* », la Commission devra être consulté en amont.

424. Ce cadre contraignant limite en grande partie les velléités d'interconnexion de la part des principaux gestionnaires de bases de données. Cependant, grâce à de nombreuses innovations apparues ces dernières années dans la gestion de celles-ci, les facilités techniques leurs ont redonné un certain attrait. Pour pouvoir juger de la légalité de ces traitements innovants, il faudra procéder à un examen technique de ces technologies, à l'instar de l'analyse de la Cour Allemande sur les plugins sociaux[734].

425. Toutefois, il faut également prendre en compte la finalité des traitements. Des traitements différents peuvent avoir une même finalité déclarée : la valorisation des données. Dans cette optique, suivant la doctrine de la CNIL, une simple déclaration sera suffisante si les données d'origine sont accompagnées du consentement initial de la personne concernée pour un tel transfert. Dans ce système, on peut observer qu'une nouvelle fois, seul le consentement autorise réellement l'interconnexion, la déclaration n'intervenant qu'à titre informatif.

733 Ibid.
734 LG Düsseldorf, Urteil vom 09/03/2016, Az.: 12 O 151/15.

Conclusion

426. Nous avions observé dans la première section que le consentement relevait d'une obligation juridique et économique. Dans cette seconde section, nous avons démontré que le consentement était utilisé pour légitimer une collecte des données bien supérieure à ce que le service a besoin pour son fonctionnement. Celui-ci légitime la collecte de l'ensemble des données utilisateurs, d'une grande partie des données que son appareil va collecter et des sites tiers, par interconnexion ou par la mise en place de plugins sociaux.

114. Cela semble remettre en question la valeur du consentement de l'utilisateur ainsi que l'efficacité de la protection édifiée par le régime. En effet pour certains auteurs, cette structure « *conduirait à une sur-responsabilisation des acteurs, qui ne tiendrait compte ni de la complexité du contexte technologique dans lequel ceux-ci évoluent, ni des situations de déséquilibre structurel, voire de la vulnérabilité auxquelles les acteurs font face lorsqu'ils sont censés consentir* »[735]. En somme, la dépendance de la protection des données au consentement conduirait les GAFA à obtenir grâce au consentement initial une main mise plus importante sur les données, alors même que les personnes concernées seraient dépendantes de l'accès au service.

115. Or, cette procédure sert également à déterminer le champ d'utilisation des données. En donnant son consentement, l'utilisateur n'autorise pas seulement le responsable de traitement à collecter ses données, il permet dans le même temps à celui-ci de les exploiter dans les conditions définies. Afin d'évaluer l'efficacité de la protection, il convient donc d'analyser celles-ci au regard de la procédure du consentement initial.

735 Lazaro Christophe, Le Metayer Daniel, *Le consentement au traitement des données personnelles : une perspective comparative sur l'autonomie du sujet*, Revue juridique Thémis de l'Université de Montréal, voi.48 n°3, 2015, p 2.

Chapitre 2

La place centrale du consentement dans la valorisation des données

*

427. Nous avons précédemment constaté la nécessité de recourir au consentement pour débuter un traitement de données. Cependant, la vie du traitement ne s'arrête pas à la collecte des données. C'est pourquoi dans ce second chapitre, nous allons nous attacher aux processus de valorisation des données. En effet, c'est à l'intérieur de ces derniers que se loge la véritable capacité du service à s'imposer face à ses compétiteurs et à développer un modèle économique viable.

428. Pour cela, il nous faudra d'abord comprendre dans quelle mesure l'innovation numérique dépend de la faculté de valoriser les données (Section 1), en observant concrètement le fonctionnement de certains d'algorithmes utilisés par les GAFA. Cela nous amènera à nous pencher sur les nouvelles méthodes de valorisation des données et en particulier sur les technologies API (Section 2), devenues aujourd'hui un standard incontournable dans l'innovation.

Section 1

Une innovation technique dépendante de la valorisation des données

429. Nous avons précédemment relevé qu'un traitement de données issue de l'innovation numérique était dépendant juridiquement du consentement. Cependant, nous n'avions pas examiné à quel point l'innovation numérique était techniquement dépendante de celui-ci. Car c'est aujourd'hui un fait, les différents algorithmes de traitements possèdent une puissance inégalée dans l'histoire. Capables de compiler des milliers de données, les « *data scientists* »[736] assistés de différents programmes sont capables de prédire les comportements humains, d'associer des centres d'intérêt à un utilisateur, voire d'aller jusqu'à la création de nouvelles informations pour produire de nouveaux services. Or dans ce contexte, l'acquisition de données n'est plus le seul facteur de réussite pour le développement de ces services face aux capacités de valorisations des données. L'enjeu n'est donc pas d'obtenir une masse considérable de données, mais de savoir s'en servir.

430. Pour observer cela, nous verrons tout d'abord un exemple de traitement de données à travers l'un des plus performant actuellement, celui de Google (1). Nous observerons ensuite de quelle manière Facebook se sert de ces procédures de traitement pour améliorer ses services (2). Cela nous permettra de mettre en avant le fait que ces nouveaux types de traitements nécessitent des infrastructures déterritorialisées, posant un problème juridique de par la domiciliation des données (3). Cette focale nous servira de base pour démontrer que c'est bien le consentement qui reste le facteur de légitimité ultime pour les traitements et l'avenir de l'innovation numérique.

736 v. Lemberger Pirmin, Batty Marc, Morel Médéric, Raffaelli Jean-Luc, *Big Data et Machine Learning : Manuel du Data Scientist*, Dunod, 18 février 2015, 240 p.

1 – Exemple d'un large traitement de données : Google

431. Il n'est pas aisé d'obtenir des informations sur la mécanique interne des géants du web. Les algorithmes de traitements constituent un avantage en termes d'efficacité technique et de valorisation, et demeurent un secret industriel face aux concurrents. Il faut donc passer par une approche indirecte, en observant les finalités déclarées des traitements. Celles-ci, devant être en accord avec les déclarations faites à l'utilisateur, apportent un début de réponse quant à la structure interne des traitements. Ainsi, s'il nous est impossible de nous pencher sur les détails techniques des algorithmes dont Google souhaite garder le secret[737], on peut s'approcher de leurs fonctionnements en observant leurs objectifs déclarés dans les conditions générales de service.

432. En l'espèce pour Google, la finalité déterminée est celle de « *fournir, gérer, protéger et améliorer nos services, d'en développer de nouveau, et de protéger aussi bien nos utilisateurs que nous-même* »[738], mais également de « *proposer des fonctionnalités personnalisées sur les produits, telles que des résultats de recherche personnalisés, des publicités sur mesure, et la détection de spams et de logiciel malveillants* » [739]. Si la seconde formulation est assez précise pour comprendre la destination des données extraites, la mention portant sur l'amélioration et la gestion des services nécessitait une explication.

433. Pour cela, Google signale que ce type de traitement correspond à une utilisation de données dans un cadre différent. Ainsi, *« le correcteur orthographique de Google a été développé à partir de l'analyse de recherches précédentes que les internautes avaient eux-mêmes corrigées* » [740]. C'est donc la totalité de l'interaction de l'utilisateur avec le service de Google qui est analysée, compilée et comparée aux données à caractère personnel identifiant la personne. Dans ces termes, on peut distinguer deux types d'utilisations distinctes des données à caractère personnel. D'une part, le service cherche à identifier la personne avec un maximum de précision pour lui proposer une interface personnalisée en fonction de ses gouts

737 Spiegle Online, *Sorge vor Kartell : Maas hatte gerne, dass Google geheime Suchformel offenlegt*, Spiegle Online, 16.09.2014, http://www.spiegel.de/wirtschaft/unternehmen/google-heiko-maas-fordert-offenlegung-von-algorithmus-a-991799.html (consulté le 01/09/2017).
738 Règles de confidentialité de Google, version du 19 Août 2015, p3.
739 Ibid. p3.
740 Ibid. p8.

et habitudes ainsi qu'à obtenir une valorisation potentielle maximale des données pour les annonceurs. D'autre part, il s'agit de comprendre le cheminement de l'utilisateur à travers les services, simplement à travers sa manière d'utiliser les pages ou même les entrées de son clavier.

434. Cette seconde utilisation est à mettre en parallèle avec l'ensemble des données que le service collecte. En l'espèce, l'exemple du traducteur construit à partir des entrées des utilisateurs est révélateur de la faiblesse de définition de la finalité des traitements pour ce type d'utilisation. À l'instant de la collecte, l'utilisateur ne sait pas quelle sera la destination des informations qu'il a fournies. Plus encore, on peut s'interroger sur la connaissance même que Google a de l'utilisation de ce type de données lors de leurs collectes. La construction du traducteur était-elle envisagée lors de la première collecte ? Si tel est le cas, la rédaction peut être, pour le moins, qualifiée d'imprécise en ce qui concerne le traitement exact et la destination des données qui sont captées.

435. Dans tous les cas, on peut constater que les finalités déclarées couvrent un large pan du domaine informatique : ciblage de l'utilisateur, cybersécurité, en passant par la création de « *nouveaux* » algorithmes. Dans ce contexte, le traitement efficace des informations devient une nécessité non pas juridique mais technique. En s'offrant la possibilité, dans les finalités déclarées, de traiter les données à des fins d'amélioration de ses services, Google obtient un avantage sur ses concurrents en fournissant un service plus personnalisé à ses utilisateurs. Sous certains aspects, on peut donc considérer que les aspects juridiques liés à la déclaration des finalités ont pour but de pérenniser les investissements des GAFA relatifs à l'attractivité de leurs propres plateformes. La valorisation sort ici de sa dimension purement économique, pour revêtir un intérêt pour les utilisateurs, à travers une fluidité accrue dans l'utilisation des services et une meilleure intégration des nouveaux arrivants.

436. Pour arriver à cette fin, les GAFA utilisent aujourd'hui de nouveaux algorithmes capables de traiter des données en provenance de sources hétérogènes, à l'instar de ce Facebook semble indiquer dans ses conditions générales.

2 – Un croisement des données fournies par les utilisateurs sur les utilisateurs : l'exemple de Facebook

437. Au cœur de cette guerre de l'information et de la course à la valorisation, on peut trouver les algorithmes d'agrégations. Ces derniers sont capables d'associer une information à un individu, sans que celui-ci l'ait fournie directement. Pour cela, ils se servent d'un réseau de captation étendu dont Facebook est aujourd'hui l'un des leaders.

438. Ainsi, le réseau social agrège les données que les utilisateurs fournissent, à la fois lors de leur propre utilisation du service, mais aussi à travers les différents capteurs présents sur le téléphone (GPS, Wi-Fi, Bluetooth) que l'application est en mesure d'exploiter. Ces informations concernent l'utilisateur, mais peuvent également contenir des données sur d'autres personnes avec lesquelles il pourrait être en contact. Captées par Facebook, celles-ci vont nourrir le profil d'une personne sans qu'elle en ait été avertie en amont, posant une nouvelle fois la question du respect du consentement et de la licéité du traitement. Sont par exemple concernés « *les contenus et informations que les autres personnes fournissent lorsqu'elles ont recours à nos Services, notamment des informations vous concernant, par exemple lorsqu'elles partagent une photo de vous, vous envoient un message ou encore lorsqu'elles téléchargent, synchronisent ou importent vos coordonnées* »[741]. Cette seconde source d'informations vient enrichir le profil détaillé que Facebook détient, alors même que les paramètres dédiés au contrôle de la confidentialité ne permettent pas de s'opposer à ce type de traitement.

439. Dans de ses pages dédiées à la configuration du profil, Facebook précise : « *vous ne pouvez pas empêcher quelqu'un de vous identifier dans une publication qui inclut un lieu, mais vous pouvez éviter qu'elle n'apparaisse dans votre journal* »[742]. La possibilité de retirer cette identification n'existe qu'à posteriori et demeure d'un effet relatif : « *Les identifications supprimées n'apparaissent plus sur la publication ou la photo, mais ces dernières restent visibles par les personnes avec qui elles ont été partagées. D'autres utilisateurs peuvent avoir*

741 Facebook, Politique d'utilisation des données, version datée du 30 janvier 2015, disponible sur https://fr-fr.facebook.com/about/privacy (consulté le 01/09/2017).
742 Facebook, Politique d'utilisation des données, version datée du 30 janvier 2015, disponible sur https://fr-fr.facebook.com/about/privacy (consulté le 01/09/2017).

la possibilité de voir cette publication ou la photo en d'autres endroits, tels que le fil d'actualité ou les résultats de recherche » [743]. Pour que cette suppression soit parfaitement effective, il faudra demander « *à la personne qui l'a publiée de la retirer* » [744].

440. Ce faisant, le réseau social effectue un renversement de la responsabilité du contrôle des publications en se déchargeant de la suppression effective sur l'utilisateur à l'origine de la publication. D'un point de vue juridique, on peut rapprocher ce mécanisme de la responsabilité limité des hébergeurs. Le réseau social conserve sa procédure de vérification des publications par rapport aux « *standards de la communauté* », qui détaillent les types d'informations qui peuvent être censurées (propos haineux, menaces etc.) mais crée une zone grise à l'intérieure de laquelle l'utilisateur n'est plus maître de la publicité des informations qui le concernent. Cela peut constituer une double contrainte pour la personne concernée. D'une part une information la concernant est accessible aux autres utilisateurs sans son consentement. D'autre part le traitement automatique des algorithmes va interpréter cette information, venant nourrir son profil de publicités ciblées.

441. Dans cette configuration, nous sortons du régime mis en place par la décision de la Cour Européenne dans l'affaire Lindqvist[745]. En l'espèce, une personne avait mis sur le site internet de sa paroisse des informations sur ces membres, ainsi que des données permettant de les contacter. Cette publication a été faite sans leur consentement, et indiquait des informations particulièrement sensibles, comme la mention d'une blessure au pied d'une personne ayant entrainée un congé de maladie partiel. La Cour va considérer que « *L'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations relatives à leurs conditions de travail et à leurs passe-temps, constitue un «traitement de données à caractère personnel, automatisé en tout ou en partie,» au sens de l'article 3, paragraphe 1, de la directive 95/46 /CE du Parlement européen et du Conseil […]* ». Ainsi, il est logique que Facebook tente de faire basculer la responsabilité sur

743 Facebook, Pages d'aide, Comment puis-je supprimer une identification d'une photo ou d'une publication dans laquelle je suis identifié(e), disponible sur https://www.facebook.com/help/140906109319589 (consulté le 01/09/2017).

744 Facebook, Pages d'aide, Comment puis-je supprimer une identification d'une photo ou d'une publication dans laquelle je suis identifié(e), disponible sur https://www.facebook.com/help/140906109319589 (consulté le 01/09/2017).

745 CJCE, *6 novembre 2003, Bodil Lindqvist*, aff. C-101/01.

l'utilisateur ayant divulgué l'information. Pourtant, celui-ci traitera la donnée de la même façon que s'il avait acquis le consentement initial.

442. Ce traitement automatique est d'ailleurs étendu aux discussions privées. Lorsqu'un échange entre deux ou plusieurs personnes est détecté par la plateforme, les algorithmes vont analyser les messages pour y repérer certains mots clés qui serviront à adapter la publicité contextuelle[746]. Cette technologie est présente dans d'autres services de messageries, à l'instar de la solution Gmail développée par Google, qui a reconnu son utilisation pour adapter les publicités au profil de l'utilisateur : « *notre système automatisé analyse le contenu (y compris des emails) afin de personnaliser l'affichage des différents services, les résultats de recherche, des publicités ciblées, ainsi que pour la détection de spam et de malware. Cette analyse débute lorsque le consentement est envoyé, reçue et enregistré* »[747]. Cette source d'information sur l'utilisateur est analysée puis traitée selon différents algorithmes qui peuvent aller jusqu'au repérage d'activités frauduleuses.

443. Selon Jon Sullivan, ancien chef de la sécurité de Facebook, le réseau social a également développé un algorithme qui, à partir de plusieurs critères, comme la proximité géographique, la différence d'âge et la fréquence des messages, est capable de détecter les potentiels pédophiles[748]. Lorsque le logiciel signale un comportement suspect, les équipes de Facebook accèdent à la discussion et décident si un signalement aux autorités est envisageable. Ce système est actif en France et a conduit à une première condamnation à partir de son signalement[749].

444. Cependant, l'utilisateur n'a pas de maitrise sur les messages qui lui sont envoyés. La suppression des messages est possible, mais « *la suppression d'un message ou d'une*

746 v. *Campbell et al v. Facebook Inc*, Filing 202, Answer to Second Amended Complaint by Facebook Inc, Jessen, Joshua, Filed on 6/28/20116, Modified on 6/26/2016, VlkS, Court Staff.

747 Traduction par l'auteur de: « *Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored* ». Google Terms of Service, Last modified April 14, 2016, disponible sur http://www.google.com/intl/en/policies/terms/ (Consulté le 01/09/2017).

748 Menn Joseph, *Social Networks can Scan for Sexual Predators, with uneven results*, Reuters, 12 July 2012, disponible sur http://www.reuters.com/article/us-usa-internet-predators-idUSBRE86B05G20120712 (consulté le 01/09/2017).

749 AFP, *Jean-Luc Lahaye condamné à un an de prison avec sursis*, Le Figaro, 18 mai 2015, disponible sur http://www.lefigaro.fr/musique/2015/05/18/03006-20150518ARTFIG00101-proces-de-jean-luc-layahe-le-verdict-tombe-ce-lundi.php (Consulté le 01/09/2017).

conversation de votre boîte de réception n'entraîne pas sa suppression de la boîte de réception de votre ami(e). Il est impossible de supprimer des messages envoyés ou reçus de la boîte de réception d'un(e) ami(e) »[750]. La construction du profil ciblé par les algorithmes, allant même jusqu'à la détection d'activités suspectes et la lecture des échanges, est alors tributaire du comportement de l'utilisateur tiers envoyant un message. Dans ces conditions, le périmètre de la collecte et du traitement est-il encore légitimé par le consentement initial de l'utilisateur ? Nous tenterons d'y répondre dans le second titre de cette partie.

3 – Une valorisation transnationale des données

445. De nombreux services numériques utilisent les réseaux transnationaux afin d'amener les données dans les data center de leurs choix, facilitant ainsi les procédés de valorisation. En concentrant les données acquises, ceux-ci sont en mesure d'extraire ou d'agréger un plus grand nombre d'informations. Or, il existe une sphère de protection qui entoure les données Européennes. Si celles-ci peuvent circuler librement entre les 27 Etats membres pour une même entité, l'article 25 de la directive 95/46/CE[751], repris en grande partie par les articles 44 et suivants du RGPD fixe des limites quant aux transferts vers les pays tiers[752]. Ainsi, à l'exception de l'Islande, du Liechtenstein et de la Norvège, qui ont transposés la directive en droit interne[753] : « *un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale [ne] peut avoir lieu [que] lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminées dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat* »[754]. Le principal facteur de licéité de ces transferts va donc reposer sur la validité de l'accord de reconnaissance de la protection adéquate des données.

750 Facebook, Pages d'aide, Comment supprimer des messages ou une conversation, disponible sur https://fr-fr.facebook.com/help/192631610782421 (consulté le 01/09/2017).

751 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

752 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 44.

753 v. Commission Nationale de l'Informatique et des Libertés, *Les transferts de données à caractère personnel hors Union Européenne*, novembre 2012.

754 Règlement (UE) n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016, Op. Cit., article 45.

446. Pour juger de cette adéquation, la Commission analyse « *toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées* » [755]. Cependant, afin de faciliter le cadre d'échange de données, l'article 25 autorise également la Commission à engager des négociations spécifiques pour garantir ce niveau de réciprocité dans l'exercice des droits de la personne.

447. Le Safe Harbor fut le résultat de ces négociations bilatérales entre la Commission Européenne et les Etats Unis, conclues par la décision de la Commission datée du 26 juillet 2000[756]. Celle-ci crée un cadre juridique protecteur dérogeant au régime général, et permet de transférer des données Européennes aux Etats Unis sous la condition que les entreprises effectuant de tels transferts adhèrent aux principes du Safe Harbour et s'enregistrent auprès du département du commerce Américain chaque année. Ce système s'appuie essentiellement sur l'auto-certification des entreprises, conditionné par le respect du droit des données, et par un contrôle réalisé outre-Atlantique par la Fédéral Trade Commission. Cette délégation ne prive pas pour autant les autorités nationales de mesures à l'encontre des entreprises Américaines, qui restent soumises au droit Européen et peuvent faire l'objet d'interdictions de transferts ciblées. En 2013, le Safe Harbour s'appliquait aux 3246 entreprises Américaines enregistrées au département du commerce Américain[757].

448. Ce pilier juridique d'une grande partie de l'économie numérique reposant sur la faculté de collecter des données sur un continent pour les valoriser sur des serveurs distants fut remis en cause par l'arrêt du 6 octobre 2015 de la Cour de Justice de l'Union

755 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, article 25.

756 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour PrivacyPrinciples and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000, page 7

757 Commission Européenne, *Communication from the Commission to the European Parliament and the Council, on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM/2013/847 Final, Brussels, 27 November 2013, p. 4.

Européenne[758]. En l'espèce, la Cour a considéré que « *si le recours, par un pays tiers, à un système d'auto certification n'est pas, par lui-même, contraire à l'exigence prévue à l'article 25, paragraphe 6, de la directive 95/46, selon laquelle le pays tiers concerné doit assurer un niveau de protection adéquat en raison de [la] législation interne ou [des] engagements internationaux» de ce pays, la fiabilité d'un tel système, au regard de cette exigence, repose essentiellement sur la mise en place de mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner, en pratique, d'éventuelles violations des règles assurant la protection des droits fondamentaux, notamment du droit au respect de la vie privée ainsi que du droit à la protection des données à caractère personnel* »[759].

449. De plus, « *la décision 2000/520 consacre la primauté des exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis sur les principes de la sphère de sécurité, primauté en vertu de laquelle les organisations américaines auto-certifiées recevant des données à caractère personnel depuis l'Union sont tenues d'écarter, sans limitation, ces principes lorsque ces derniers entrent en conflit avec ces exigences et s'avèrent donc incompatibles avec celles-ci* »[760]. Ainsi, constatant qu'il existe aux Etats Unis certaines législations autorisant l'accès aux données par les autorités étatiques pour des raisons de sécurité nationale, ce niveau de protection adéquat n'était pas assuré, ce qui justifiait une annulation de la décision fondatrice du Safe Harbour.

450. Celui-ci fut remplacé par un nouvel accord nommé Privacy Shield[761] malgré les nombreuses critiques émanant du G29[762]. Mais il semble que d'un point de vue juridique ce nouvel accord ne puisse subsister. En effet, si l'on prend en compte l'analyse de la Cour de Justice ayant conduit à l'annulation du premier accord, la législation Américaine autorisant les services de renseignement à accéder aux données est toujours en vigueur, et donc, menace de la même manière la licéité de la décision fondatrice de ce nouveau régime.

451. L'ensemble de l'économie numérique ne saurait reposer sur un tel risque juridique. Dès lors, la totalité des GAFA ont fait usage de l'exception présente à l'article 49 de la

758 CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14.
759 Ibid.
760 Ibid.
761 Commission Européenne, *Communiqué de Presse*, IP/16/2016, Strasbourg, 2 février 2016.
762 Groupe de Travail « Article 29 » sur la protection des données *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft adequacy decision, Adopted on 13 April 2016*, 16/EN, WP 238.

directive 95/46/CE, autorisant le transfert lorsque la personne a donné son consentement. Cette exception a d'ailleurs été fortement réduite dans le RGPD, puisqu'auparavant il était nécessaire d'informer la personne concernée de l'absence des garanties appropriées[763], alors que le règlement général ne fait plus mention de cette obligation d'information[764]. Par défaut, c'est donc encore une fois l'exception basée sur le consentement aux conditions générales de services qui va légitimer les traitements à une échelle internationale.

Conclusion

452. Le recours aux conditions générales est un moyen pour les responsables de sécuriser juridiquement leurs traitements de données personnelles et constitue un moyen simple de s'auto-attribuer une liberté presque totale sur le champ des données collectées, leurs utilisations, et leurs domiciliations. En définissant eux-mêmes ces différents éléments, les services s'extraient des principales limitations du cadre général, en particulier concernant la sphère de protection définie dans l'espace Européen, en se servant de l'exception prévue par le consentement de la personne.

453. Cela s'applique aux principaux algorithmes de valorisation, qu'il s'agisse simplement d'améliorer les fonctionnalités de leurs services, ou ceux chargés de collecter et traiter les données. Au cœur de cette structure, le consentement devient un outil de légitimation crucial pour l'innovation technologique, à tel point que son intégration se fait de manière de plus en plus systématique au niveau technique, à l'instar de ce que l'on peut observer dans les technologies API, devenues aujourd'hui incontournables pour les acteurs du numérique.

763 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, article 49.

764 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, article 49.

Section 2

Une valorisation portée par les nouvelles capacités des APIs

454. Devenues incontournables, les Interfaces de Programmations Applicatives[765] sont des outils logiciels mis à disposition par certains services informatiques pour faciliter l'accès à leurs bases de données par des services tiers. Celles-ci répondent à un problème technique récurent dans l'informatique qui découle des différences de codes et de logiciels utilisés pour la gestion des bases de données, rarement compatibles entre eux. En générant une API, le service crée une interface unique qui sert de zone mitoyenne entre ces différents langages. Il n'est plus nécessaire pour un programme « *consommateur* » de connaitre la structure interne de la base « *fournisseur* », mais simplement d'intégrer cette API qui se chargera de traduire les requêtes et de formuler les réponses correspondantes.

455. Cela crée un schéma de requêtes stratifiées avec une logique simplifiée pouvant s'apparenter au rôle d'un traducteur. Le logiciel client formule une requête et l'envoie à l'API qui la traduit pour le logiciel fournisseur. La réponse suit alors le chemin inverse, facilitant l'interaction. Un second avantage réside dans la capacité du créateur à définir précisément cette interface et l'accès qu'elle propose. Ce faisant, le développeur peut masquer la structure de la base de données interrogée ainsi qu'une grande partie de ses données tout en fournissant une réponse adaptée. Au final, le service est en mesure de créer différents types d'accréditations, permettant de limiter ou d'augmenter les possibilités d'interactions avec la base sans avoir à la fournir dans son intégralité. C'est donc l'outil idéal pour valoriser de l'information. Cependant, il nous faut définir la structure du régime juridique qui s'y applique.

456. Pour cela, nous verrons tout d'abord comment les APIs constituent les nouveaux outils d'interaction des bases de données (1), et comment celles-ci sont devenues un moyen de contrôle de l'information (2). Suivant ces observations, nous pourrons étudier le régime applicable aux APIs (3), ainsi que la répartition de la responsabilité (4) en leur sein. Enfin, nous verrons les différentes règles techniques auxquelles elles sont soumises (5).

765 En anglais: « *Application Programming Interface* ».

1 – Les APIs : nouveaux outils d'interaction des bases de données

457. Les APIs sont très utilisées par les sites internet proposant de comparer les prix, puis de réserver un vol en ligne. L'utilisateur entre ses préférences de vols dans une boite de dialogue, puis, les APIs intégrée des différentes compagnies aériennes relaient la requête jusqu'à leur base de données afin de trouver une correspondance. Les résultats sont ensuite affichés directement sur la page sans que le client ait à interroger indépendamment chaque compagnie. Pour l'agence de voyage, cela permet de proposer un grand nombre de vols sur une page web unique, et pour les compagnies aériennes, cela permet d'accroitre leurs périmètres de ventes respectifs.

458. Ce faisant, ces nouveaux moyens d'accéder aux bases de données de services tiers autorisent parfois l'accès à des données à caractère personnel. Elles sont même devenues des portes d'entrée vers des milliers de profils et informations divers sur les utilisateurs des réseaux sociaux. En balayant les obstacles techniques liés à l'acquisition de données, les APIs ont permis l'émergence de nouvelles sociétés dédiées à la capture et à la monétisation des données à caractère personnel présentent sur les principaux réseaux sociaux.

459. Pour étudier ce phénomène, nous allons nous pencher sur l'API la plus utilisée au monde, celle donnant accès à la plus grande base de données utilisateurs existante : Facebook Graph. Le site vient récemment de dépasser les 1.7 Milliards d'utilisateurs actifs par mois[766]. Il reste le premier exemple de réussite de cette technologie appliqué à l'information sociale et ce succès est dû en partie au développement de son API qui permet à des sociétés tiers d'accéder aux données de ses utilisateurs[767]. Facebook Graph se présente comme : « *l'interface principale par laquelle les applications peuvent lire et écrire sur le graphe social de Facebook* » [768].

766 Statista, The Statistics Portal, *Number of monthly active Facebook users worldwide as of 2nd quarter 2016 (in millions)*, Statista, Disponible sur http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (consulté le 01/09/2017).

767 v. Définition de l'API Facebook Graph, disponible sur https://developers.facebook.com/docs/graph-api?locale=fr_FR (Consulté le 01/09/2017).

768 Ibid.

460. Ce « *graph social* » constitue la représentation technique des informations que le réseau détient sur ces utilisateurs. Sa définition est d'une grande importance puisque la structure utilisée est reproduite dans la plupart des bases de données utilisateurs à travers le monde. Celle-ci est constituée de « *nœuds* », éléments ou objets identifiables indépendamment comme un utilisateur, une photo, une page ou un commentaire. Elle associe à ces « *nœuds* » des « *arrêtes* » qui schématise les liens entre ces différents objets. À titre d'exemple, un commentaire se retrouve lié à une photo par celles-ci. Enfin, elle associe un « *champs* » à ces éléments, permettant d'ajouter des attributs à un nœud comme une date de naissance ou une date de création.

461. Pour les développeurs, elle reste « *le meilleur moyen d'insérer et de récupérer des données dans la plate-forme de Facebook. Il s'agit d'une API HTTP de bas niveau qui vous permet d'interroger des données, de publier de nouvelles actualités, de gérer des publicités, de télécharger des photos et de réaliser différentes autres tâches qu'une app peut être amenée à effectuer* »[769]. En fonction de divers paramètres, les applications externes vont pouvoir acquérir des données précises sur les utilisateurs, et ensuite valoriser ces informations par des accords de publicité. Cela peut aller jusqu'au profil complet de l'internaute, de la religion déclarée de la personne à ses sports préférés, en passant par les terminaux qu'il utilise pour accéder au service et sa localisation[770].

462. Ouverte aux développeurs en 2007[771], l'API ne constitue pas pour autant un flux ouvert vers les données des utilisateurs. Elle ne répond aux requêtes qu'à la condition que celles-ci soit formulée par une application associée au service et en lien avec l'utilisateur. Par conséquent, il est nécessaire pour un développeur de faire reconnaitre son application et d'intégrer le code source de l'API dans son propre code. Parfaitement intégrée, celle-ci devient visible par l'utilisateur final de l'application et s'affiche comme une partie importante de l'expérience utilisateur. Elle emporte par la même occasion une partie des contraintes liées au réseau social, en rendant l'inscription ou l'authentification obligatoire pour profiter de toutes les fonctionnalités.

769 Ibid.

770 On peut trouver une liste complète sur le site des développeurs de Facebook, disponible sur https://developers.facebook.com/docs/graph-api/reference (Consulté le 01/09/2017).

771 Arrington Michael, *Facebook Launches Facebook Platform,* TechCrunch, 24 Mai 2007, disponible sur https://techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/ (Consulté le 01/09/2017).

463. Mais en rendant obligatoire l'inscription à Facebook pour accéder à un logiciel, le réseau social gagne de nouvelles audiences, et les développeurs d'applications peuvent s'appuyer sur l'infrastructure du réseau social, sans avoir à créer de nouveaux outils. Les développeurs y trouvent un moyen d'améliorer leurs visibilités en profitant des fonctions de partages, et les utilisateurs une façon unique de s'authentifier sur différentes applications. Aujourd'hui disponible sur différentes plateformes (web, Google Android, Apple iOS), l'application est donc devenue incontournable pour de nombreux logiciels.

2 – Les APIs : moyens de contrôle et d'acquisition de l'information

464. La décision de développer une API pour un service n'est pas neutre. Celle-ci relève d'une véritable politique commerciale et de contrôle sur les informations échangées. Lorsqu'un service atteint une taille suffisante, il peut être opportun de développer une solution logicielle en interne à destination des logiciels clients, plutôt que de laisser croitre une myriade de moyens externes d'accès à sa base de données. Facebook a réussi ce tour de force. En proposant très tôt un système, le réseau social a jugulé le déploiement de solutions tierces. Les développeurs d'applications ont progressivement adopté son API dans leurs codes, et les utilisateurs ont pris l'habitude de se servir de ces moyens d'authentifications et de partage de contenus.

465. Ce faisant, le réseau acquiert un contrôle total sur le principal moyen d'interagir avec ses utilisateurs. Il est libre ensuite de dicter les différentes accréditations conditionnant l'accès, qu'elles soient gratuites ou payantes. Cela confère un double avantage.

466. Tout d'abord, l'opérateur de l'API est capable d'établir les conditions juridiques applicables. En soumettant l'accès à l'API à celles-ci, le service impose un cadre de responsabilité dans l'utilisation des données. Grace à la contractualisation de l'accès, Facebook limite donc sa responsabilité à l'égard des tiers, et engage celle des logiciels clients. Ensuite, le réseau conserve la maitrise technique d'une application cruciale dont il peut modifier le code à tout instant. Ces modifications servent d'ailleurs de grille de lecture pour comprendre l'évolution du réseau, dans sa dimension technique et juridique, que l'on peut

retrouver lorsque l'on effectue une recherche dans les nombreuses modifications ayant eu lieu ces dernières années.

467. Enfin, l'intégration de l'API permet, comme on l'a vu avec les plugins sociaux[772], de disposer de nouveaux terrains pour recueillir de l'information sur les utilisateurs. En proposant ce service dans les pages internet et dans les applications, Facebook étend ses capacités de collecte. Ainsi, Blizzard, l'un des plus grands éditeurs de jeux vidéo au monde vient de signer un partenariat avec la firme Californienne pour associer ses jeux au réseau social[773]. D'un côté, l'éditeur pourra proposer des interactions sociales enrichies à ses joueurs et profiter des services de streaming de la plateforme pour toucher un public plus large. De l'autre, Facebook gagne un accès privilégié à des millions de joueurs et à leurs données d'activités. Ces types de partenariats se multiplient, et la place des APIs dans le développement n'a jamais été aussi forte.

468. Les APIs sont un moyen de contrôler le flux d'informations échangées entre un service et ses clients ainsi que d'étendre ses capacités de collecte. Dès lors, il nous appartient de qualifier le régime applicable, aussi bien du point de vue du service qui développe ce type de solution, que de celui des clients accédant aux données.

3 – Le régime applicable aux APIs

469. En premier lieu, il faut s'assurer de la légalité de la base de données initiale. C'est le régime classique lié au traitement de données à caractère personnel mis en place par la loi informatique et libertés qui s'applique[774]. Sa définition a déjà été étudiée dans la partie I titre I

772 « *Applications liées aux différents médias ou réseaux sociaux (Facebook, Twitter, Youtube, Viadeo, etc..) qui peuvent être placées sur un site tiers par un simple copier / coller de code fourni par la plateforme sociale. Pour le site d'accueil, les plugins sociaux peuvent permettre notamment de proposer la recommandation de contenus, d'utiliser des données de profils pour des commentaires, l'enregistrement ou la complétion de formulaires ou d'afficher des contenus en provenance des sites sociaux ».* Bathelot Bertrand, *Définition: Plugins sociaux*, Définitions Marketings, Encyclopédie illustrée du marketing, 28 juillet 2015, disponible sur http://www.definitions-marketing.com/definition/plugins-sociaux/ (consulté le 01/09/2017).

773 Génération NT*, Blizzard mise sur le streaming sur Facebook,* Génération NT, 7 juin 2016, disponible sur https://www.generation-nt.com/blizzard-accord-streaming-facebook-actualite-1929576.html (consulté le 01/09/2017).

774 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004, Article 3.

chapitre II section I de cet ouvrage, et n'appelle pas de commentaire spécifique quant à son applicabilité lors de la constitution d'une base de données composée de données à caractère personnel. Cependant, des particularités juridiques dérivant du développement d'une API apparaissent à l'instant où celle-ci est mise à disposition de développeurs tiers.

470. Ainsi, sa définition technique va revêtir une importance capitale au moment de l'examen de la responsabilité de son fournisseur et de ses clients. L'entité qualifiée sera en charge de mettre en place les différentes mesures assurant un niveau de protection efficace, tout en s'assurant de la conformité du traitement avec les finalités déclarées initialement. Or, il peut exister une certaine confusion autour de la notion de traitement dans les technologies APIs. Souvent initiées par le fournisseur, les opérations sur les données se sont déroulées en amont du partage pour les ordonner à l'intérieur d'une base intelligible et exploitable. Une seconde série d'opération est alors être effectuée par le client de l'API, qui va de nouveau transformer ces données pour les valoriser. Si d'un point de vue technique ces opérations peuvent se distinguer, il peut exister dans la pratique juridique une réunion de celles-ci sous une qualification et une responsabilité unique à travers la notion de traitement.

471. La notion juridique de traitement de données à caractère personnel s'applique de manière uniforme, sans prendre en compte les différentes étapes logicielles employées pour traiter les données. Qu'il s'agisse d'une collecte, d'une analyse ou bien de la simple sauvegarde de données, la définition regroupe *« un ensemble d'opérations ou tout ensemble d'opérations »*[775] sous une même appellation. Pourtant, pour analyser la licéité d'un traitement, le régime impose une lecture temporelle des conditions de licéité. À ces différentes étapes correspondent différentes mesures juridiques qualifiant la responsabilité et les mesures nécessaires à appliquer. L'appréciation de la licéité d'une API doit donc être accompagnée d'une analyse de facto de la succession des opérations réalisées.

472. Dans le cas des APIs, une analyse sur trois niveaux est possible, en suivant la stratification complexe des opérations techniques reliant un fournisseur de données, ses clients professionnels et ses utilisateurs. Pour cela, on peut distinguer respectivement : la

775 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 2.

collecte auprès des utilisateurs initiaux, le don et les formalités d'accès données aux clients de l'API, et enfin, la capture de nouvelles informations à travers le déploiement de celle-ci. À l'intérieur de ces différentes strates, il faudra appliquer les règles particulières relatives à la sécurité des données, au respect du consentement de la personne, ainsi que leurs implications techniques. Pour cela, il nous appartiendra de considérer un exemple hypothétique d'API qui transfère des données à caractère personnel, justifiant l'application du régime de la loi informatique et libertés[776].

473. À chacune de ces étapes, les éléments juridiques vont nécessiter une transcription technique particulière pour s'adapter au régime de protection et garantir la licéité de l'API et de son utilisation. Cependant, avant d'analyser les mesures spécifiques, il nous faut rappeler qu'en cas de traitement de données à caractère personnel la responsabilité échoit au responsable de traitement. Or, « *la notion de responsable de traitement des données et son interaction avec la notion de sous-traitant des données jouent un rôle central dans l'application de la directive 95/46/CE, car elles déterminent la ou les personnes chargées de faire respecter les règles en matière de protection des données et la manière dont les personnes concernées peuvent exercer leurs droits dans la pratique* » [777].

474. Cette articulation est particulière puisqu'il existe une pluralité d'acteurs intervenant dans le traitement des données. Le service initial, collecteur des données les traitant pour son propre compte et offrant un accès d'une partie de celles-ci à ses clients, réalisant à leurs tour leurs propres traitement. Par conséquent, il faudra dans un premier temps déterminer si la particularité de l'usage des APIs peut être qualifiée de traitement unique sur le plan juridique, ou bien si ces opérations sont distinctes avec une pluralité de responsables de traitements.

475. Selon l'article 3 de la loi informatique et libertés, le responsable de traitement est «*sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses*

776 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 2.

777 Groupe de Travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* Adopté le 16 février 2010, 00264/10/FR, WP 169, p. 2.

finalités et ses moyens » [778]. Cette formulation, associée à l'alinéa 2 de l'article 3[779], permet d'éviter qu'en cas de sous-traitance, la responsabilité soit diffusée à un organisme tiers qu'y n'effectuerait les opérations que pour le compte de l'organisme collecteur des données. En effet, « *le responsable ne doit pas être confondu avec les personnes qui, tels les employés ou les sous-traitants, mettent en œuvre des traitements pour son compte* » [780].

476. Cependant, la loi conditionne l'applicabilité de cette responsabilité limitée au respect des conditions fixées par l'article 35 de la loi de 1978 : « *Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi* ». *Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement* » [781]. Afin de faire la distinction entre un sous-traitant et un responsable, le G29 a mis en place trois critères de qualification : la capacité d'agir, celle de déterminer les finalités et les moyens, et le degré d'autonomie dans cette décision[782].

778 Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés***,** modifiée par la Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,* Publiée au Journal Officiel du 7 août 2004. Article 3.

779 « *Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données* ». Ibid.

780 Turk Alex, *Rapport n°218 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, Annexe au procès-verbal de la séance du 19 mars 2003, p. 49.

781 Ibid. Article 35.

782 Groupe de Travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* Adopté le 16 février 2010, 00264/10/FR, WP 169.

4 – La répartition de la responsabilité dans l'exploitation d'une API

477. Tout d'abord, il faut savoir que celui qui « *détermine* » les finalités du traitement en devient le responsable. On doit donc nécessairement décomposer en premier lieu cette capacité d'agir. Faisant une référence explicite à la convention 108 qui le définissait comme « *le maître du fichier* »[783], le groupe de travail indique que le responsable était celui « *qui est compétent […] pour décider* »[784]. Cependant, par l'utilisation de la capacité de « *détermination* » plutôt que de celle de « *compétence* », la directive Européenne, et a fortiori, la formulation de la loi de 1978, s'extrait de l'analyse juridique du pouvoir de la structure pour s'attacher aux éléments factuels de la décision d'entreprendre le traitement, licite ou non. Le comité précise que la désignation contractuelle du sous-traitant ou du responsable ne lie pas le juge dans l'appréciation de cette qualité. Ainsi, « *la notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle. Par conséquent, un examen long et approfondi sera parfois nécessaire pour déterminer cette responsabilité* »[785].

478. La notion de « *personne* » s'entend ici au sens large, qu'elle soit morale ou physique. Ce qui importe c'est l'amplitude donnée à une entité pour prendre cette décision. Un employé agissant pour le compte de son employeur ne pourra être désigné responsable individuellement. Par contre, à l'instar de la jurisprudence dédié à la responsabilité du préposé, celle-ci pourra être engagée s'il a agi en dehors du cadre de sa mission, même sans intention[786].

479. En appliquant cette analyse à la technologie des APIs, on peut attribuer cette capacité au service fournisseur ainsi qu'au service client, qui peuvent être liés contractuellement, mais qui ne sont pas dans une relation préposé / employeur. Il faut donc appliquer le second critère : celui de la détermination de la finalité et des moyens. Pour cela, le G29 énonce que

783 Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, Article 2.
784 Ibid.
785 Groupe de Travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* Adopté le 16 février 2010, 00264/10/FR, WP 169, p. 10.
786 Cass. Crim., 27 mai 2014, n°13-80849, Bull. Crim. 2014, n°137.

« *lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable de traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant* » [787].

480. En cela, il apparait que le fournisseur est doublement libre. D'une part, il dispose de toute sa liberté quant à la définition de la finalité lors de la collecte de sa base de données. Celle-ci étant généralement réalisée en amont du développement d'une API, la détermination de la finalité ne saurait être du ressort du client. Toutefois, dans le cas où un service déciderait, en concertation avec son client, de réaliser une collecte pour son compte et de lui fournir une API facilitant l'accès à la base, devenant ainsi un simple intermédiaire technique, la responsabilité de la détermination de la finalité échouerait sur le client final de l'API.

481. Associé à la définition de la finalité, la définition des moyens peut apporter une clarté supplémentaire dans la désignation du responsable de traitement. Le G29 résume son intérêt ainsi : « *alors que la détermination de la finalité du traitement emporterait systématique la qualification de responsable du traitement, la détermination des moyens impliquerait une responsabilité uniquement lorsqu'elle concerne les éléments essentiels des moyens* » [788]. C'est finalement dans le degré d'autonomie dans la conception technique de l'API que va se nicher la qualification du responsable de traitement. La façon dont les données sont partagées, et dans quels but celles-ci ont été collectée va définir un régime de responsabilité, applicable soit au client, soit au fournisseur, ou bien encore, créer un régime de co-responsabilité en fonction des détails techniques interne de l'application. Or, il existe certaines règles techniques aux portées juridiques qui sont applicables lors de la conception d'une API.

787 Groupe de Travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* Adopté le 16 février 2010, 00264/10/FR, WP 169, p. 14.
788 Idib, p15.

5 – Les règles techniques applicables à la conception d'une API

482. En complément des dispositions législatives, un certain nombre de définitions techniques sont apparues afin de transcrire les obligations du responsable du traitement en termes opérationnels. Celles-ci se sont progressivement développées à la suite d'une série d'usages controversés de la technologie, à l'instar de Facebook Beacon[789]. En l'espèce, Facebook proposait à des sites partenaires d'installer une API sur leurs pages. En échange de la présence de l'algorithme, le site internet offrait une opportunité pour son visiteur de publier son achat sur son compte Facebook en direct. Dans le même temps, le réseau social enregistrait la navigation de l'utilisateur et était en mesure de proposer une publicité ciblée en fonction de l'historique de navigation et d'achat.

483. La publication des actions sur un site tiers était automatique et exposait certaines actions de l'internaute directement sur le réseau social, visibles par l'ensemble de ses contacts. Le système reposait sur une procédure d'opt-out pour la publication, qui pouvait être supprimée à posteriori du profil. Mark Zuckerberg déclarait : « *Au départ nous avons essayé de l'alléger afin que les personnes n'aient pas à y toucher pour que celui-ci fonctionne. Le problème de notre approche initiale basée sur un système d'Opt Out, plutôt que sur un système d'Opt In, était que si une personne oubliait de décliner cette option, Beacon envoyait quand même cette information et la partageait avec ses amis* »[790]. Une class-action fut immédiatement lancée aux Etats Unis par des utilisateurs de Facebook mécontents que leur navigation soit publiée sans leur accord. Celle-ci eut pour effet d'imposer au réseau social une

789 Pour une description complète, on peut se référer à celle donnée par le jugement dans l'affaire Lane v. Facebook. Ainsi, en anglais, celle-ci décrit le système ainsi : « *Facebook described the purpose of the Beacon program as allowing its members to share with friends information about what they do elsewhere on the Internet. The program operated by updating a member's personal profile to reflect certain actions the member had taken on websites belonging to companies that had contracted with Facebook to participate in the Beacon program. Thus, for example, if a member rented a movie through the participating website Blockbuster.com, Blockbuster would transmit information about the rental to Facebook, and Facebook in turn would broadcast that information to everyone in the member's online network by publishing to his or her personal profile* ». Lane v. Facebook, Inc, 709 F.3d791, 9 Circ.2013, 20 septembre 2012.

790 Traduction par l'auteur de : « *At first we tried to make it very lightweight so people wouldn't have to touch it for it to work. The problem with our initial approach of making it an opt-out system instead of opt-in was that if someone forgot to decline to share something, Beacon still went ahead and shared it with their friends* ». Mark Zuckerberg, *Thoughts on Beacon*, 5 décembre 2007, disponible sur https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130 (Consulté le 01/09/2017).

refonte anticipé de l'application avec un système d'opt-in et de créer une nouvelle modalité pour la désactiver complètement[791].

484. Une affaire similaire eut lieu en Europe l'année suivante. Cette fois, l'API n'était pas à destination des internautes, mais autorisait une compagnie privée, Phorm, à capter le trafic internet des clients de certains fournisseurs d'accès d'outre-manche en accédant directement à leurs bases de données[792]. Cela lui permettait ensuite d'afficher des publicités ciblées sur son réseau de bannières apposées sur les sites internet partenaires. Basée une nouvelle fois sur un système d'opt-out, la controverse a conduit la commission Européenne à lancer une enquête, s'inquiétant des phases de tests ayant eu lieu en amont du déploiement officiel[793]. Celle-ci nourrira les réflexions entourant la création de la directive 2009/136/CE, renforçant l'obligation de consentement préalable au stockage et à la lecture d'information sur le dispositif de l'utilisateur[794].

485. Ces deux exemples posent une première distinction à effectuer lors de l'examen de la licéité d'une API, achoppant notamment sur la méthode retenue pour identifier l'utilisateur. D'une part, nous avons une API qui utilise l'authentification à un réseau social pour justifier l'utilisation des informations récupérées sur un site tiers. De l'autre, nous avons une exploitation conjointe des données de connexions, fournies par le fournisseur d'accès, et des cookies présents sur des sites partenaires. Or, conformément à la directive 2009/136/CE, si une technologie utilise en partie les cookies du navigateur, le recueil du consentement de l'internaute sera nécessaire en amont. Les différents outils mis à la disposition des professionnels pour effectuer ce recueil doivent être mis en place, à l'instar du modèle mis en place par la Commission Européenne[795], ainsi que celui de la CNIL[796].

---

791 Ibid.

792 Waters Darren, *EC starts legal action over Phorm*, BBC News website, disponible sur http://news.bbc.co.uk/2/hi/technology/7998009.stm (Consulté le 01/09/2017).

793 Commission Européenne**,** *Telecoms: Commission launches case against UK over privacy and personal data protection*, IP/09/570, Brussels, 14 April 2009.

794 Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009, *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal Officiel de l'Union Européenne n°L337/11, 18 décembre 2009.

795 Disponible sur http://ec.europa.eu/ipg/design/templates/commission/index_en.htm (Consulté le 01/09/2017).

796 Disponible sur https://www.cnil.fr/fr/exemple-de-bandeau-cookie# (Consulté le 01/09/2017).

486. Dans le cas contraire, la question du respect du consentement reste à analyser. En effet, lors de la collecte de données réalisées pour le traitement initial, il est nécessaire de détailler l'utilisation ultérieure des données. Cependant, cette description est limitée à la définition des technologies existantes, sans inclure nécessairement les possibilités supplémentaires d'utilisations du service apportées par les APIs. La personne peut être confrontée à un nouveau logiciel, et les implications en termes de vie privée seraient alors subordonnées à sa maitrise du système. L'exemple de Facebook Beacon en est révélateur. En souscrivant aux conditions générales de service, les utilisateurs avaient juridiquement donné leur consentement à l'utilisation des données par l'API, dans les conditions qui étaient définies. Cependant, la publication des informations de navigation sur le profil dépassait ce consentement, au moins dans sa dimension concrète. L'analyse de la technologie API nécessite donc de s'extraire de la dimension purement juridique de la licéité du consentement, pour s'attacher à définir l'expression de la volonté de la personne. En cela, les règles techniques deviennent indispensables pour compléter l'arsenal juridique dédié à la protection de la vie privée.

487. Selon le World Wide Web Consortium : « *les considérations de vie privée sont importantes pour les APIs, étant donné que l'utilisation frauduleuse d'information exposées par celles-ci peuvent avoir des conséquences financières, physiques, de réputation et bien plus encore* »[797]. En conséquence, la protection de la vie privée « *a besoin d'une solution systémique incluant des fonctionnalités définies pour les utilisateurs, les sites internet et les autres composants du système, puisque chacune des opportunités offertes par les possibilités d'utilisation frauduleuse constitue un risque* »[798]. Fort de son pouvoir de normalisation technique, le W3C a mis en place une série de règles applicables au développement de l'API et à ses moyens d'interaction avec l'utilisateur : les Device API Privacy Requirements[799]. Il utilise pour cela deux types d'exigences, l'une obligatoire : DOIT, l'autre préférable mais facultative : DEVRAIT.

797 Traduction par l'auteur de: « *privacy considerations are important to Device APIs, since misuse of information exposed by the APIs can have potentially harmful financial, physical safety, reputational and other impacts* ». World Wide Web Consortium, Device API Privacy Requirement, W3C Working Group, Note 29 June 2010

798 Traduction par l'auteur de: « *needs a systemic solution that includes functional requirements on user agents, web sites and other components of the system, since any opportunity for misuse of private information is a risk* ». Ibid.

799 Ibid.

488. Ainsi, l'API DOIT proposer un moyen d'information sur les données collectées, ainsi qu'identifier avec précision l'application en question. Celle-ci DEVRAIT proposer un support visuel pour faciliter cette compréhension. L'API DOIT faire en sorte de recueillir un consentement explicite, et à défaut, limiter les conditions dans lesquelles l'interprétation de ce consentement peut être implicite lors de l'exécution d'une opération. Le logiciel DOIT également faire en sorte que l'accès aux données puisse être limitatif, et en lien aux opérations nécessaires. Il DOIT proposer une façon pour l'utilisateur de révoquer son consentement. Enfin, les APIs DOIVENT intégrer un mécanisme à destination des utilisateurs pour exprimer leurs préférences vis-à-vis de l'utilisation premier et secondaire des données, ainsi qu'à destination de leurs clients pour prolonger leur propre politique d'utilisation des données.

489. Ces principes seront précisés dans une nouvelle note de juin 2012[800], en rappelant notamment l'importance de la « *minimalisation des données* » [801] dans le déploiement d'une API. Celui-ci propose d'utiliser des paramètres de confidentialité contextualisés, plutôt qu'une application demande l'ensemble des permissions pour accéder à toutes les données lors de la première utilisation.[802]. Cela permet de réduire au minimum l'accès aux données lors du recueil du consentement de l'utilisateur, tout en laissant l'application les utiliser de manière sporadique à des moments différents. Toutefois, cette dernière mesure reste une recommandation sans valeur juridique.

800 World Wide Web Consortium, Patterns for Privacy by Design in Javascript APIs, W3C Draft Tag Finding, 6 June 2012.

801 « *Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur* ». Saltzer Jerome, Schroeder Michael, *The protection of Information in Computer Systems*, CS551, Security and Privacy on the Internet, 17 April 1975.

802« *At first sight this appears to conflict with the requirement that users be asked to make direct privacy decisions as little as possible, but there is a subtle distinction at play. Direct privacy decisions will prompt the user to provide access to information at the application's behest, usually through some form of permissions dialog. User-mediated access will afford a control for the user to provide the requisite information, and do so in a manner that contextualises the request and places it in the flow of the user's intended action ».* World Wide Web Consortium, Patterns for Privacy by Design in Javascript APIs, W3C Draft Tag Finding, 6 June 2012.

Conclusion

490. En accélérant fortement sa croissance, Facebook a généré une nouvelle façon de concevoir les APIs. Autrefois réservées aux arcanes du développement informatique, celles-ci sont devenues l'un des outils les plus en vogue actuellement. Le succès du bouton « *like* », présent sur plus de dix millions de site internet en est la preuve[803]. La plateforme déploie depuis quelques années cette nouvelle forme d'interaction avec sa base de données utilisateurs, devenant une technologie incontournable pour la plupart des services dématérialisées qui interagissent avec les citoyens. Toutefois, cela n'est qu'un exemple parmi d'autre. Les GAFA se sont progressivement armés dans cette guerre de collecte d'information, en développant toujours plus ces nouvelles technologies pour un contrôle étendu des entités tierces avec qui ils traitent. En cela, les APIs sont un outil incontournable du web 2.0 et du big data de demain dans leur façon d'interconnecter les services et les bases de données.

491. Pour autant, cette évolution ne se produit pas hors de toute règlementation juridique ou technique. Le régime applicable aux données à caractère personnel prolonge une grande partie de la protection de la vie privée jusqu'à ces nouveaux usages, et sa traduction en termes techniques et en termes d'acceptabilité sociale a été assurée par le W3C. Ainsi, on peut constater, en observant les changements introduits dans l'API Graph de Facebook, l'histoire de la protection des données de ces dernières années, ainsi qu'anticiper ces futures évolutions.

492. Tout d'abord, on remarque que la plateforme s'est rapidement dotée d'un règlement spécifique, applicable à l'utilisation de son API[804]. Il fait une référence directe au respect des standards de la communauté, relatif aux informations publiables, ainsi qu'aux règles publicitaires spécifiques[805]. Le réseau social a également intégré les recommandations du W3C[806]. D'une part, il demande aux applications tiers d'obtenir *« le consentement des personnes avant de publier du contenu en leur nom »* [807], marquant ainsi un tournant face à au

803 Zephoria, *Top 20 valuable Facebook Statistics,* Juillet 2016, disponible sur https://zephoria.com/top-15-valuable-facebook-statistics/ (consulté le 01/09/2017).
804 Règlement de la plateforme Facebook, disponible sur https://developers.facebook.com/policy/#control (consulté le 01/09/2017).
805 Ibid. Article 1.
806 World Wide Web Consortium, *Device API Privacy Requirement*, W3C Working Group, Note 29 June 2010
807Règlement de la plateforme Facebook, Article 2. disponible sur

développement de ses premières balises[808]. De même, il impose la rédaction d'une politique de confidentialité accessible aux utilisateurs. Afin de s'assurer de la licéité du traitement de son API, Facebook a effectué une mise à jour conséquente de son application le 30 avril 2014[809]. Autrefois plus permissif, le logiciel intégra dans son code les recommandations juridiques et techniques liés aux API. Ainsi, les utilisateurs seront libres de choisir de transférer ou non les informations demandées à l'application tierce. Enfin, les informations données de façon automatiques ne seront plus celles du profil complet, mais celles du profil public de l'utilisateur.

493. En plus de ces mesures, une boite de dialogue automatique sera générée, demandant la permission pour l'application d'accéder aux données de l'API. Cette permission sera différente selon les applications en accord avec les principes de minimalisation des données, en demandant une permission spécifique à chaque catégorie d'informations. Grace à un système de « *token d'accès […] chaine opaque qui identifie un utilisateur, une app ou une page, et que l'app peut utiliser pour passer des appels de l'API Graph* » [810], Facebook est capable de surveiller les différents accès de sa base, et contrôler la légitimité des applications qui y ont recourt.

494. À cause de ses qualités, l'API Graph constitue un exemple réussi de l'intégration des recommandations techniques et juridiques à l'intérieur du fonctionnement d'une API, tout en y ajoutant la mise en place de limites techniques de partages de données liées à l'acceptabilité sociale. Facebook sera en mesure d'assurer la conformité de son propre traitement avec les finalités qu'il a déterminées lors du recueil du consentement de l'utilisateur grâce à la maitrise technique qu'il détient sur l'API. De plus, il instaure une responsabilité distincte pour le tiers client de l'API. Pour cela, il fait appel au consentement de l'utilisateur, qui va devenir un élément fondateur du second traitement. Ce faisant, Facebook force l'application d'un régime de protection à double responsabilité de traitement, la sienne, et celle de son client. Le logiciel devient pour lui non seulement une interface technique avec les tiers, mais également un filtre

https://developers.facebook.com/policy/#control (consulté le 01/09/2017).

808 Notamment, Facebook Beacon, v. pont 127 de cet ouvrage.

809 Voir API Graph Changelog note, April 30th 2014, API Version v2.0. Disponible sur https://developers.facebook.com/docs/apps/changelog#v2_0 (Consulté le 01/09/2017)

810 Facebook Developers, Tokens d'acces, disponible sur https://developers.facebook.com/docs/facebook-login/access-tokens/ (Consulté le 01/09/2017).

juridique l'isolant des possibles infractions aux réglementations réalisées par ses clients sur ses données.

495. Toutefois, d'après ses propres conditions : « *Nous pouvons analyser votre application, votre site web, votre contenu et vos données dans n'importe quel but, y compris commercial* » [811]. Dès lors, il parait plus difficile de limiter le traitement de Facebook à son API, alors même que celui-ci va également enregistrer les données qui transitent par l'application tierce. Il peut ainsi suivre l'activité de son utilisateur, même si celui-ci pensait être sous un second régime de protection. Pour savoir si celui-ci est licite, il faudra une nouvelle fois se référer aux conditions de services initiales, décrivant les finalités et les moyens du traitement. Or, comme nous l'avons vu, celles-ci sont souvent opaques.

496. Dans ce premier titre, nous avons pu ainsi observer un double phénomène. D'abord, il existe une obligation juridique et technique qui ne cesse de se renforcer pour que le consentement soit la base légitime de tout traitement. Ensuite, cette structure renforce le pouvoir des services pour obtenir la légitimation de collectes et de traitements étendus à des fins de valorisations économiques. À travers les conditions générales de services, les responsables de traitement crées eux même le maillage juridique auquel ils seront soumis, maillage qu'il étende grâce à leurs avancées technologiques. Sur ce point, on peut d'ailleurs observer une relative homogénéisation des conditions générales à travers les différentes plateformes présentes en Europe[812], ainsi que des développements algorithmiques similaires, notamment en ce qui concerne les APIs. Cela conduit à une forme de vampirisation des services tiers par les GAFA, appuyée autant par la technologie que par le droit, allant jusqu'à une soumission presque systématique des différents terminaux utilisés pour accéder aux services.

497. Or, l'ensemble de cette structure économique et technique repose sur le consentement et fait peser une menace sur la protection de la vie privée que Daniel Solove qualifie de perte du contrôle de l'utilisateur sur ses données[813]. Ainsi, ce n'est pas directement la technologie

811 Règlement de la plateforme Facebook, Article 6. disponible sur https://developers.facebook.com/policy/#control (consulté le 01/09/2017).

812 v. Rogosch Patricia, Hohl Erik, *Data Protection and Facebook: An Empirical Analysis of the Role of Consent in Social Network,s* LIT Verlag, 10 octobre 2012, 72 p.

813 *« Privacy self-management takes refuge in consent. It attempts to be neutral about substance — whether*

qui porte une atteinte à la protection de la vie privée, mais la façon dont le régime s'appuie sur le consentement. Maintenant que ce fait est établi, et que les traitements légitimés paraissent sans commune mesure avec l'intérêt direct d'accéder à un service, il nous appartient de savoir dans quelle mesure la protection est effectivement érodée par ce principe du consentement initial.

certain forms of collecting, using, or disclosing personal data are good or bad — and instead focuses on whether people consent to various privacy practices. Consent legitimizes nearly any form of collection, use, or disclosure of personal data. Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data ». Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, p. 141.

Titre II

Une protection érodée par le recours au consentement

*

498. En liant la protection de la vie privée au consentement, le régime cherche à placer l'individu au centre de la légitimité du traitement de données afin qu'il puisse décider, pour lui-même, la latitude qu'il souhaite accorder au responsable de traitement. Selon le G29, « *s'il est utilisé à bon escient, le consentement est un instrument qui permet à la personne concernée de contrôler le traitement de ses données* » [814]. Pourtant, nous avons constaté l'existence d'un décalage important entre les objectifs de protection du régime, son application dans les faits, et une procédure de recours au consentement qui justifie des traitements et des acquisitions de données très étendus. En cela, l'intégration du consentement parait détournée de son objectif initial et le contrôle de la personne concernée sur ces données semble devenir illusoire.

499. Cela montre qu'il peut exister une dichotomie entre la volonté réelle de la personne concernée et la « *manifestation de volonté indubitable* »[815] exprimée lors de la procédure de recueil du consentement aux conditions générales de service. En se rattachant à un consentement défini par le droit, le régime semble avoir rationalisé une notion soumise à la controverse de l'interprétation des comportements humains et de leur authenticité dont les critères de validités sont aujourd'hui exploités par les GAFA. Pour expliquer cette dichotomie, il convient tout d'abord de préciser que le consentement juridique possède une valeur binaire, positive ou négative, considérant la volonté et le consentement comme des éléments nécessairement convergents.

814 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 2.

815 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

500. Ainsi d'un point de vue juridique, si le consentement est donné, c'est que la volonté de l'individu y est nécessairement associée. Pourtant dans les faits, il existe une véritable distinction entre ces deux notions. Pour Alicia-Dorothy Mornington : « *le consentement se distingue de la volonté car il s'inscrit dans une relation préexistante, il constitue une réponse à une proposition ou à un ordre. Le registre de la volonté, comme celui du souhait, ne dépend pas nécessairement du contexte, puisqu'il s'agit du projet d'un agent qui peut vouloir de manière indépendante sans que sa volonté soit une réponse à une proposition extrinsèque* »[816]. Elle prend l'exemple du cadre médical dans lequel le consentement du patient recueilli avant une opération n'est pas nécessairement l'expression d'une volonté de subir l'acte, mais l'assentiment à un moyen de réduire sa maladie. Nombreux sont ceux qui ne souhaitent pas vraiment subir un acte chirurgical, mais qui y consentent malgré tout devant l'absence d'autres options.

501. La même logique est transposable aux traitements de données à caractère personnel. Les individus, bien que consentants, ne sont pas toujours en accord profond avec l'usage qui va être fait de leurs données alors même qu'ils s'y engagent sur le plan juridique. Si l'on souhaite effectivement que les citoyens aient le contrôle de leurs données, il convient d'analyser les mécanismes qui régissent cette procédure, et de tester leur capacité à laisser s'exprimer fidèlement la volonté des personnes.

502. Pour cela, il faut comprendre qu'il existe essentiellement deux difficultés. La première est d'ordre matériel : une personne aura une grande difficulté à lire, puis à comprendre les implications directes des conditions générales de service auxquelles elle souscrit. Selon Aleecia McDonald et Lorrie Faith Cranor, qui ont calculé l'exposition moyenne d'un internaute aux conditions générales de service sur une année, il faudrait environs 201 heures par an, soit plus de huit jours complets pour les lire entièrement[817]. Ensuite, en admettant qu'un utilisateur prenne le temps de parcourir les différentes clauses avant de signifier son accord, on peut exprimer une réserve sur le pouvoir supposé de compréhension des clauses juridiques, parfois absconses, ou au moins de leurs implications pour une personne qui n'est

816 Mornington Alicia-Dorothy, *La Fiction du Consentement dans les Relations Asymétriques entre Employé et Employeur,* La langue du management et de l'économie à l'ère néo-libérale : formes sociales et littéraires, textes réunis par Corinne Grenouillet et Catherine Vuillermot-Febvet, Presses Universitaires de Strasbourg, coll. Formes et Savoirs, 2015.

817 McDonald Aleecia, Cranor Lorrie Faith, *The Cost of Reading Privacy Policies*, I/S: A journal of Law and Policy for the Information Society, 2008.

pas familière du droit. Pour Daniel Solove, « *même si la plupart des personnes lisait les règles de confidentialité régulièrement, ils manquent souvent d'une expertise suffisante pour analyser avec précision les conséquences de l'acceptation de celles-ci au regard des utilisations présentes ou des transferts futurs de leurs données* »[818].

503. La seconde difficulté est d'ordre sociologique. Un grand nombre d'études dans le champ des sciences sociales remettent en cause la capacité du consentement à être un bon instrument juridique, notamment à travers la mise en évidence des biais cognitifs qui peuvent être utilisés pour fausser le jugement d'un individu et le conduire à contracter en dépit de ses propres intérêts[819]. Ces études remettent en cause deux croyances habituellement associées à la volonté : celle qui laisse penser que l'individu est toujours le maître exclusif de ses décisions en l'absence de violence ou de contrition directe, et celle qui tend à affirmer le fait qu'il prend toujours la meilleure option pour lui-même. Ainsi : « *les travaux en science sociale – que je pourrais définir rapidement comme comprenant l'étude des comportements économiques, psychologiques et empiriques dans d'autres domaines – montrent que la plupart de nos assomptions à propos de la façon dont les personnes prennent des décisions sont fausses. Comme les professeurs Richard Thaler et Cass Sunstein le notent : « la fausse impression que presque toutes les personnes, presque tout le temps, font des choix qui sont en accord avec leur intérêt ou du moins, font de meilleurs choix que si ceux-ci étaient fait pas d'autres »* [820] »[821].

818 Traduction par l'auteur de: « *even if most people were to read privacy policies routinely, people often lack enough expertise to adequately assess the consequences of agreeing to certain present uses or disclosures of their data* ». .Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, p. 148.

819 On peut citer notamment le champ de l'économie cognitive, qui se situe à la croisée de la théorie des jeux se basant sur des analyses décisionnelles stratégiques de la part de l'acteur, et de la théorie des échanges dans laquelle les acteurs ont des croyances. v. Walliser Bernard, *Economie et Cognition*, Editions Odile Jacob, 25 Août 2008, 263 p.

820 v. Thaler Richard H, *Nudge: Improving Decision About Health, Wealth and Happiness*, Penguin, 24 février 2009, 320 p.

821 Traduction par l'auteur de: *« Work in social science — which I will define broadly to encompass behavioral economics, psychology, and empirical studies in other fields — shows that so many of our cherished assumptions about the way people make decisions regarding privacy are false. As Professors Richard Thaler and Cass Sunstein note, the "false assumption is that almost all people, almost all of the time, make choices that are in their best interest or at the very least are better than the choices that would be made by someone else » ».* Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, p. 148.

504. Ces considérations dérivent de la réflexion débutée par Daniel Kahneman dans le champ de l'économie comportementale[822], et qui expose « *le caractère faux de l'idée traditionnelle d'un modèle de décision humaine rationnel, alors même que la plupart des personnes se décident en fonction de l'heuristique et de la manière dont les choix sont exposés* » [823]. Or, à cette imperfection humaine vient se heurter à la précision juridique. Les conséquences du don du consentement peuvent être extrêmement importantes pour un individu dans le domaine de l'innovation technologique. Les profils en ligne deviennent publics, les informations sont échangées, et à partir d'un simple clic, l'individu devient le sujet de dizaines de traitements différents, ou ses données seront vendus à des plateformes de publicités ciblés.

505. Pour pallier ces difficultés, le régime a progressivement intégré des mesures tendant à s'assurer de la qualité du consentement. Bien qu'absente de la loi informatique et libertés, la définition du consentement issue de l'article 2 dans la directive 95/46/CE indique que celui-ci consiste en « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* » [824]. Il convient de définir ces éléments et de qualifier ce que l'on entend par leur respect dans la procédure de consentement aux conditions générales de service, afin de vérifier si cet instrument juridique est toujours pertinent dans sa forme actuelle, et s'il intègre avec justesse les réflexions issues de la science cognitive.

506. Pour répondre à cette problématique, nous nous proposons d'étudier ces éléments constitutifs dans le cadre de la relation asymétrique qui unit utilisateur et responsable de traitement (Chapitre 1). De ces premières observations, nous pourrons déduire les conséquences d'une remise en cause générale de la validité du consentement (Chapitre 2).

---

822 v. Kahneman Daniel, *Thinking Fast and Slow*, Penguin, 10 mai 2012, 512 p. ; Kahneman Daniel, Amos Tversky, *Choices, Values and Frames*, American Psychologist, April 1984, pp. 341-350 ; Kahneman Daniel, Slovic Paul and Tversky Amos, *Judgment under Uncertainty, Heuristic and Biases*, Cambridge University Press, 20 mai 1982, 544 p.

823 Traduction par l'auteur de: « *the falsity of the traditional rational agent model of human decisionmaking, as people often decide based on heuristics and the way choices are framed* ». Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, p. 148.

824 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

Chapitre 1

La remise en cause de la validité du consentement dans une relation asymétrique

*

507. Si la question du respect de la volonté de l'utilisateur dans l'innovation technologique doit être posée, c'est nécessairement dans son cadre d'application concret, c'est à dire dans la procédure de recueil du consentement aux conditions générales de service. En effet, s'il existe d'autres modes de légitimation pour développer des traitements de données à caractère personnel, le consentement reste le principal facteur juridique sur lequel s'appuie l'économie numérique. Celui-ci fonde la licéité des traitements de données ayant un objectif de valorisation, modèle économique choisi par les principaux acteurs numériques. Qu'il s'agisse de créer un profil sur un réseau social tel que Facebook ou bien de simplement installer une application sur son smartphone, l'utilisation est systématiquement conditionnée à l'acceptation préalable de ce type d'accord.

508. Comme nous l'avons observé, cet écosystème révèle une double dépendance dont le consentement est le pivot. D'une part, l'utilisateur doit obligatoirement accepter ces conditions s'il souhaite accéder au service. D'autre part, le service à besoin de ce consentement pour valoriser les données acquises, cette activité étant à la base de son modèle économique. Des lors, la rédaction des conditions générales, ainsi que la façon dont le consentement est recueilli sont déterminantes. En cela, l'analyse de sa validité dépasse l'intérêt du citoyen seul, mais touche également la sécurité juridique de l'économie numérique

509. La Commission Européenne souligna cette double dépendance dans sa communication datée de novembre 2010, en relevant plusieurs difficultés structurelles : « *Dans un environnement en ligne – vu l'opacité des politiques de protection de la vie privée -, les personnes ont souvent plus de difficulté à s'informer sur leurs droits et à donner un consentement éclairé. Cela est d'autant plus complexe que, dans certains cas, l'on ne voit pas clairement ce qui constituerait un consentement libre spécifique et éclairé à un traitement de données, comme dans le domaine de la publicité comportementale en ligne ou certains considèrent, mais pas d'autres, que les paramètre du navigateur de l'internaute expriment son consentement* » [825]. C'est donc dans ce contexte que le G29 lança entre 2010 et 2011 un programme de travail tendant à « *clarifier la situation afin de garantir une compréhension commune du cadre juridique existant* »[826] dont les résultats seront publiés dans son avis 15/2011 sur la définition du consentement.

510. Dans cet avis, le G29 va s'attacher à donner des définitions plus précises des critères associés au consentement tels que la liberté, la spécificité et l'information suffisante ; avant de s'intéresser à la manière dont on peut le recueillir. Cela va constituer les éléments fondateurs de la licéité du consentement, sans pour autant remettre en cause la structure de la relation contractuelle qui va se créer entre un utilisateur et un service. Or, comme nous l'avons observé précédemment, celle-ci tend à légitimer des traitements de données très étendus en termes de captations et de finalités, qui vont à l'encontre des objectifs du régime.

825 Commission Européenne, *Une approche globale de la protection des données à caractère personnel dans l'union Européenne*, COM/2010/0609 final, Bruxelles, 4 novembre 2010.

826 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 2.

511. Pour étudier cette structure contractuelle, nous passerons d'abord en revue les éléments fondateurs de la licéité du traitement (Section 1) tels que définis par le G29, avant de les appliquer de manière concrète à la relation qui lie un utilisateur et un service pour déterminer la véritable valeur du consentement (Section 2).

Section 1

Les éléments fondateurs de la licéité du consentement

512. Avant de définir les éléments fondateurs de la licéité du consentement, il faut d'abord rappeler que la notion même de consentement n'est pas un concept naturel du droit. Bien que le Code Civil y consacre ses nouveaux articles 1128 et 1129, il n'est caractérisé que par la négative, en précisant les vices qui peuvent l'entacher. Il n'existe donc pas, dans la législation, de définition positive de la notion alors même que sa nature est d'une grande importance dans le cadre de notre étude sur le respect de la volonté de la personne concernée dans le traitement des données à caractère personnel.

513. Dès lors, la détermination de son essence résulte d'une réflexion doctrinale couplée à la jurisprudence qui a progressivement défini ses contours dans le cadre général. Pour le G29, « *il n'y a pas contradiction, mais bien chevauchement entre le champ d'application du droit civil et celui de la directive. En effet, la directive ne porte pas sur les conditions générales de validité d'un consentement dans le cadre du droit civil, mais elle ne les exclut pas. Cela signifie par exemple que pour apprécier la validité d'un contrat au regard de l'article 7, point b, de la directive, les conditions énoncées par le droit civil devront être prise en compte* »[827]. A l'heure où certains auteurs évoquent une dépossession du droit au respect de la vie privée au profit des GAFA, il est nécessaire de préciser son origine.

827 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 7.

514. Conceptualisée sous sa forme moderne dans la littérature des Lumières et intégrée dans le Code Civil de 1804, la notion de consentement reste liée aux réflexions du XVIIème siècle qui évoquent les droits naturels et l'idée d'une autonomie de l'Homme dans sa faculté à prendre des décisions. Selon Jean Cédras : « *pour les autonomistes, les hommes à l'état de nature sont libres. Mais raisonnables et sociaux, ils constituent la société par leur accord librement donnée. D'eux-mêmes, ils découvrent le droit naturel, à savoir ce que leur raison leur montre comme convenant à leur état social. Au rang des dogmes naturels de la vie en société se trouvent les deux idées fortes du libéralisme individualiste : celle de la liberté primordiale de l'homme et celle ramassée dans la maxime Pacta sunt servanda. […]. Le Code civil a largement repris cette théorie* »[828]. Ainsi, son ébauche résulte de la doctrine civiliste partisane de la théorie de l'autonomie de la volonté[829] et traduisant les mécanismes d'engagements contractuels des parties, où la volonté serait centrale[830].

515. Pour Francois Chénedé, celle-ci peut « *être perçue comme une théorie purement descriptive, ayant pour seule ambition de rendre compte, le plus exactement possible de la réalité observée. Mais elle peut être également comprise comme une théorie prescriptive visant, cette fois-ci, à promouvoir un certain droit des contrats, à militer pour certaines règles contractuelles* » [831]. Dès lors, il est important de comprendre que le consentement, en tant qu'instrument de manifestation de la volonté d'une partie n'est pas simplement une notion juridique pure, mais le résultat d'une certaine conception de l'engagement contractuel et de la place de la volonté de la personne dans celui-ci. Cette théorie libérale fait d'ailleurs l'objet d'une vive controverse.

516. Selon Emmanuel Gounot, la théorie de l'autonomie de la volonté s'appuie sur deux principes : Nul ne peut être obligé sans y avoir consenti et tout engagement libre est juste[832]. Or ces deux points peuvent être remis en question. Ainsi, « *la libre volonté et l'égalité sont des mythes, voire des tromperies quand les parties sont inégales en force. Sous une neutralité*

828 Cédras Jean, *Le solidarisme contractuel en doctrine et devant la Cour de Cassation*, Cour de Cassation, Rapport 2003 : l'égalité, La documentation Française, p186.
829 v. Ranouil Véronique*, L'Autonomie de la Volonté : Naissance et Evolution d'un Concept*, PUF, 1980, 165 p.
830 Jamin Christophe, *Relire Labbé et ses Lecteurs*, Archive de la Philosophie du Droit, 37, 1992, pp. 247-267.
831 Chénedé Francois, *De l'Autonomie de la Volonté à la Justice Commutative, du Mythe à la Réalité*, Annuaire de l'Institut Michel Villey, 2012, 4, p. 155.
832 Gounot Emmanuel, *Le principe de l'Autonomie de la Volonté en Droit Privé,* A. Rousseau Editeur, 1912, 470 p.

apparente, le droit classique des contrats sert en réalité de libéralisme économique et s'accommode de son cortège de duretés » [833]. Cela trouve d'ailleurs une résonnance dans le développement contractuel depuis le XIXème siècle. : « *il est en effet indéniable […] que la réalité contractuelle de 1900 n'était plus celle de 1804. Produit de l'industrialisation croissante du XIXème siècle, on vit apparaitre, à côté des classiques contrats de gré à gré, négociés par des parties aux forces équivalentes, des contrats dits d'adhésion, c'est-à-dire des conventions dont le contenu est édicté de manière unilatérale par une partie en position de force. Parmi ces contrats de masse, citons le contrat de transport (ferroviaire et maritime), le contrat d'assurance, le contrat de fourniture d'électricité et de gaz, mais également, bien sûr, le contrat de travail […]* » [834]. Dans ces nouveaux contrats, la place de la volonté fut réduite du fait de la standardisation des clauses et de l'impossibilité d'engager des négociations individuelles. Paradoxalement, la théorie de l'autonomie de la volonté va contribuer à soustraire la volonté au consentement, qui devient un outil d'engagement contractuel, plutôt que d'expression de la volonté.

517. Il existe pourtant une raison simple qui justifie en partie cette conception : si la volonté était la seule règle en matière contractuelle, celle-ci pourrait fragiliser la pérennité des obligations consenties. Pour Xavier Martin « *Si l'homme est, ainsi, conditionné par ses appétits, si la volonté n'est que girouette, des individus s'engageant par contrat doivent être, dans l'intérêt social, proprement ligotés à leur engagement, et le législateur à cet effet maintiendra dans les reins de chaque contractant la pointe de cet alinéa [Code Civil article 1134 al 1er] pour tenir socialement coordonnée cette masse d'individualités mécaniquement égoïstes* » [835]. On peut donc penser qu'en matière contractuelle, le consentement initial ne sert qu'à sanctifier un engagement plutôt qu'à exprimer sa volonté profonde. La théorie de l'autonomie de la volonté n'intervient, dès lors, que pour qualifier la période qui précède l'engagement. Avant celui-ci l'individu est libre totalement, après il est soumis aux obligations librement consenties.

518. Toutefois, cela ne vaut que si les obligations sont véritablement librement consenties. Selon Jean Cédras, avocat général à la Cour de Cassation : « *depuis la fin du XIX siècle, on*

833 Ibid. p140.
834 Ibid, p156.
835 Martin Xavier, *Nature Humaine et Révolution Française*, Martin Morin, 24 septembre 2015, p. 118.

s'est aperçu que beaucoup de contrats entre puissants et faibles n'étaient pas justes parce qu'ils n'étaient pas négociés. […]. Dans cet esprit, le législateur ou le juge ont dû entreprendre de reconstituer la solidarité naturelle entre les hommes, née de leur commune appartenance au corps social. Au profit des catégories sociales faibles, ils ont créé ou développé diverses obligations précontractuelles ou contractuelles à la charge des potentiores pour que ces derniers n'abusent point de leur situation. La loi solidariste a donc soustrait, en tout ou en partie, certains domaines à la liberté contractuelle, par exemple les retraites, la sécurité sociale, le surendettement des particuliers, la législation HLM et les baux réglementés, la consommation, etc »[836]. Cet interventionnisme relève directement de la théorie du solidarisme contractuel, qui distingue la volonté du consentement. Pour ses partisans, le consentement d'une partie faible à un contrat ne peut exprimer pleinement sa volonté. Il appartient au juge ou au législateur de rétablir cette capacité initiale à prendre la décision de s'engager, en rééquilibrant les obligations du contrat comme l'aurait fait l'individu s'il avait été à égalité avec son co-contractant. Toutefois, cet interventionnisme, à priori du législateur et à posteriori des juges, soulève les critiques classiques liées au paternalisme arbitraire des juges ainsi qu'aux risques de remise en cause de la liberté contractuelle. Cela rencontre, a fortiori, une résistance farouche des partisans de la théorie de l'autonomie de la volonté.

519. Sans chercher à prendre position sur la nature exacte du consentement en optant pour l'une ou l'autre des théories, nous pouvons constater que la définition du consentement n'est pas une notion juridique dénuée de controverse, qui est le résultat d'une certaine conception de l'engagement contractuel. Cependant, si ces deux théories divergent dans leurs analyses, elles se rejoignent sur l'importance de la place de la liberté de consentir. Il appartient dès lors, de vérifier qu'il n'existe aucun défaut dans le régime de protection relatif à cette notion, en s'attachant à définir les critères qui fondent cette liberté de consentir aux obligations et qui détermineront la capacité d'un individu à exprimer sa volonté quant à l'utilisation de ses données.

836 Cédras Jean, *Le solidarisme contractuel en doctrine et devant la Cour de Cassation*, Cour de Cassation, Rapport 2003 : l'égalité, La documentation Française, p. 187.

1 – La reconnaissance juridique du consentement dématérialisé

520. Avant de détailler les critères permettant de qualifier le consentement dans le régime applicable aux données à caractère personnel, il importe dans un premier temps de comprendre comment la manifestation de la volonté d'un utilisateur peut être recueillie juridiquement alors même que celle-ci est dématérialisée. En effet, avant le développement de l'informatique, la législation et la doctrine s'accordaient sur la reconnaissance de la signature comme preuve matérielle de la manifestation de la volonté de la partie contractante, nécessaire à la perfection d'un acte. Avec les nouveaux usages dématérialisés, la présence physique des co-contractants, qui était autrefois présupposée, n'est plus automatique. De plus, le régime applicable aux contrats à distances a été battu en brèche par la multiplication des plateformes de ventes en ligne ainsi que par la répartition géographique des grands acteurs du secteur. Il fallait donc répondre à une double difficulté : considérer le contrat électronique comme un contrat à part entière et élever le consentement dématérialisé au même niveau de reconnaissance juridique que celui accordé à la signature.

521. Pour surmonter ces deux obstacles, la Commission Européenne se lança à la fin des années 90 dans un mouvement de reconnaissance des actes conclus à distance grâce aux nouveaux moyens de télécommunication. Dans un premier temps, celle-ci s'est attachée à définir un régime Européen applicable à la signature électronique, chantier qu'elle jugeait alors prioritaire. Dès les négociations préparatoires portant sur la directive 1999/93 sur un cadre communautaire pour les signatures électroniques[837], la Commission va considérer que « *les communications et le commerce électroniques nécessitent des signatures électroniques et des services connexes permettant d'authentifier les données ; que toute divergence dans les règles relatives à la reconnaissance juridique des signatures électronique et à l'accréditation des prestataires de service de certification dans les états membres risque de constituer un sérieux obstacle à l'utilisation des communications électroniques et au commerce électronique* » [838]. Soulignant l'importance de cette prise de position, la directive, dans sa version finale, ajoutera à ce considérant : « *par ailleurs, l'établissement d'un cadre*

837 Ibid, p156.

838 Proposition de directive du Parlement Européen et du Conseil sur un cadre commun pour les signatures électroniques, COM 98/0297 final, COD 98/0191, Journal officiel n° C325 du 23 octobre 1998, p. 0005.

communautaire clair concernant les conditions applicables aux signatures électronique contribuera à renforcer la confiance dans les nouvelles technologies et à en favoriser l'acceptation générale » [839].

522. Toutefois, afin de « *trouver un équilibre entre les besoins des particuliers et ceux des entreprises* » [840], la Commission va faire la distinction entre deux niveaux de signatures électroniques différents. Ainsi, la signature électronique sera « *une donnée sous forme électronique, qui jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* » [841]. La signature électronique avancée, quant à elle, sera une signature qui satisfait aux exigences suivantes : être liée uniquement au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable. L'apport de la directive réside dans la mise en place de composés techniques pour satisfaire les exigences d'authentification de l'individu signataire, ainsi que pour assurer la sureté et la pérennité des moyens de signatures.

523. Nous pouvons observer alors que ces deux définitions, essentiellement techniques, ne couvrent finalement aucun aspect lié à la conclusion, à la validité des contrats, ou même aux autres types d'obligations légales. Il ne s'agit donc pas d'une redéfinition de la notion de consentement dans le monde numérique, mais bien d'une simple traduction des exigences d'authenticité liée à l'apposition d'une signature sur un document.

524. En se basant sur la reconnaissance de la signature numérique, il restait à la Commission à harmoniser les législations nationales concernant le contrat numérique qui contenaient « *des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique* » [842]. Elle relève à cette occasion que « *le développement des services de la société de l'information dans la Communauté est limité par un certain nombre*

839 Directive 1999/93/CE du Parlement Européen et du Conseil, du 13 décembre 1999, *sur un cadre communautaire pour les signatures électroniques*, Journal Officiel de l'Union Européenne n° L013, 19 janvier 2000, pp. 00012-0020, considérant 4.

840 Ibid. Considérant 14.

841 Ibid. Article 2.

842 Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (Directive sur le commerce électronique),* Journal Officiel de l'Union Européenne n°L178 du 17 juillet 2000, pp.0001-0016, considérant 18.

d'obstacle juridiques au bon fonctionnement du marché intérieur qui sont de nature à rendre moins attrayant l'exercice de la liberté d'établissement et de la libre prestation des services » [843]. En conséquence, selon l'article 9 de la directive 2000/31, la Commission va imposer que « *les Etats membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les Etats membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électronique ni ne conduise à priver d'effet et de validité juridique de tels contrats pour le motif qu'ils sont passés par voie électronique* » [844]. La directive s'accompagne de mesures relatives à la protection des consommateurs en matière de vente par internet, notamment en ce qui concerne l'exigence d'une information suffisante à fournir lors de la conclusion des contrats, ainsi que des détails concernant la passation des commandes.

525. En France, et avant même la directive, le législateur avait déjà anticipé cette double reconnaissance, signature et contrat, en incorporant directement une nouvelle subdivision dans la partie du Code civil dédiée au contrat. Avec la loi du 13 mars 2000 il modifia les articles 1125 et suivants afin de prendre en compte cette nouvelle forme de consentement, et lui donner « *la même force probante que l'écrit sur support papier* » [845]. Ces modifications seront d'ailleurs étendues à d'autres textes avec la loi de transposition du 21 juin 2004, dite de confiance dans l'économie numérique, dans le but d'homogénéiser les différents pans du régime[846]. Grace à cette reconnaissance, les contrats conclus par voie électronique auront la même force juridique que les contrats papiers, à condition de respecter les formalités techniques liées à la signature électronique que la directive prônait. Ainsi, selon le nouvel article 1367 du Code Civil : *« lorsqu'elle est électronique, elle [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire. Lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret au Conseil d'Etat* ». Le décret n°2001-272 du

843 Ibid. considérant 5.
844 Ibid. Article 9.
845 Loi n°2000-230 du 13 mars 2000, *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, JORF n°62 du 14 mars 2000, p. 3968, article 3.
846 Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2.

30 mars 2001, précisant ces conditions, va reprendre en grande partie les propositions de la Commission en établissant deux signatures distinctes, une simple et une sécurisée[847].

526. Si la seconde passe par un procédé technique pour s'assurer de l'identité de l'auteur, la première utilise une méthodologie d'attribution que l'on peut comparer avec celle utilisée pour authentifier les achats par carte bancaire. Ainsi, dans le cadre bancaire, il est admis que l'utilisation combinée d'une carte de crédit et du code secret associé constitue une préemption suffisante pour imputer un achat[848]. De la même manière, les sites internet seront invités à prendre le faisceau de données à leur disposition pour identifier un acheteur (adresse IP, compte, adresse, etc). Le terme « *signature* », sous sa forme classique, prend alors un sens différent. Il s'agit non plus de l'apposition d'un sceau numérique, mais d'un faisceau d'indices qui vont déterminer l'identité d'un acheteur, ainsi que sa volonté à travers une action, en l'occurrence dans le domaine commercial, celle d'effectuer un double clic pour effectuer une commande.

527. Rarement évoqué dans le cadre de la doctrine attachée à l'étude du régime applicable aux données à caractère personnel, ce développement emporte pourtant une part importante de la philosophie attaché au principal facteur de licéité des traitements : le consentement préalable. D'abord, le législateur reconnait qu'une signature numérique dispose de la même force juridique qu'une signature papier, puis il réduit sa portée dans le monde numérique par l'absence de précision technique quant à la forme que doit prendre une signature électronique simple. Ce faisant, il tente de transférer dans le monde numérique l'une des caractéristique de la formation du contrat à partir de la rencontre des volontés, qui dans le monde réel peuvent être extériorisées sans formalisme. Si l'on se réfère au régime général, le comportement de l'internaute est susceptible de caractériser l'engagement de sa volonté pour la perfection d'un acte juridique.

528. Il est aisé d'imaginer les débordements auxquels aurait conduit une utilisation très libérale de cette définition[849]. Cela fut d'ailleurs rappelé dans l'avis du contrôleur européen de

847 Décret n°2001-272 du 30 mars *2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique*, JORF n°0077 du 31 mars 2001, p. 5070.
848 CA. Montpellier, 17eme ch, sect. D, 9 avril 1987, JCP, ed. G., II, n°20984.
849 De fait, un simple clic sur un produit présenté sur un site internet marchand pourrait suffire à engager contractuellement le consommateur.

la protection des données du 14 janvier 2011 : « *Il n'est cependant pas toujours simple de déterminer ce qui constitue un consentement authentique, non équivoque. Certains responsables du traitement exploitent cette incertitude en recourant à des méthodes qui excluent toute possibilité de donner un consentement véritable, non équivoque* » [850]. Dès lors, il nous appartient de décrire quelles ont été les mesures prises afin de garantir la qualité de la manifestation de la volonté de la personne concernée.

2 – Les conditions générales de licéités du consentement

529. À titre d'observation préalable, il faut rappeler que le consentement n'a pas toujours été une notion centrale du régime applicable aux données à caractère personnel. Selon l'avis de la commission consultative sur la proposition de la Commission de la future directive 95/46/CE, qui reconnait en 1990 le développement rapide des capacités de traitement vis-à-vis de « *cette branche récente du droit* » [851], à l'époque « *seules quelques catégories particulières d'informations dont la divulgation était, en elle-même, susceptible de porter atteinte à certains intérêts de la personne physique à laquelle elles se rapportaient faisaient l'objet de mesures de protection sanctionnées juridique* » [852]. Parmi celles-ci, on ne trouve l'obligation préalable de recueillir le consentement que pour les catégories de données sensibles.

530. En effet, avant l'apparition de la directive 95/46/CE, la loi du 6 janvier 1978 se contentait d'imposer une obligation d'information de l'individu sur le traitement de ses données. Dans son article 3 celle-ci indique que « *toute personne a le droit de connaitre et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés* » [853]. Ersatz de consentement, l'obligation d'information remplaçait alors l'obligation de recueil du consentement préalable au traitement en offrant la

850 Contrôleur Européen de la protection des données, *Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions intitulée : « Une approche globale de la protection des données à caractère personnel dans l'Union Européenne* », 2011/C, Journal officiel de l'Union Européenne, 22 juin 2011, C 181/1, p. 11.

851 Commission consultative de la protection de la vie privée, Avis n°90/093 du 16 novembre 1990, Ref 10527/L/S/49, p. 2.

852 Ibid, p. 3.

853 Loi informatique et libertés, article 3.

possibilité à la personne concernée de contester les informations et les raisonnements utilisés. Le consentement était néanmoins requis, d'après son article 31, pour les données « *nominatives qui, directement ou indirectement, font apparaitre les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes* » [854]. Cependant, celui-ci ne sera généralisé en droit Français que bien plus tard, avec la loi de transposition du 6 août 2004 qui l'intègrera dans l'article 7 de la loi informatique et libertés[855].

531. Au niveau Européen, le consentement n'était pas non plus présent dans la convention 108 du 28 janvier 1981 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Celle-ci, dans son article 5, faisait référence à une obtention et un traitement « *loyal et licite* » des données[856]. Ce vide juridique relatif au niveau Européen, auquel seul l'article 8 de la Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales pouvait répondre[857], a contraint la Commission Européenne au début des années 90 à se lancer dans un chantier législatif pour introduire des mesures communautaires « *afin d'assurer la protection des individus au regard de la protection des données et pour s'assurer de la sécurité des traitement d'information dans le contexte du développement des réseaux de télécommunications* » [858].

532. Le résultat de ces réflexions se trouvera dans la directive 95/46/CE, grâce à laquelle la notion de consentement préalable entra définitivement dans le régime. Dans son article 2, celle-ci défini le consentement comme : « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement* » [859]. Si la définition parait triviale, elle

854 Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 31.

855 Loi n°2004-800 du 6 août 2004, *relative à la bioéthique*, JORF n°182 du 7 août 2004, p. 14040, texte n°1.

856 Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, article 5.

857 Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales telle qu'amendée par les Protocoles n°11 et n°14, Rome, 4 novembre 1950.

858 Traduction par l'auteur de: « *to ensure the protection of individuals in relation to the processing of personal data and to enhance the security of information processing in the context, notably, of the development of open telecommunication networks* ». Commission Européenne, *Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, Draft resolution of the representatives of the governments of the member states of the European Communities meeting within the Council*, COM/90/314 final, Brussels, 13 September 1990, p. 2.

859 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre*

s'accompagne pourtant de certaines difficultés d'interprétations. De l'avis même du G29, « *La genèse de la directive 95/46/CE fait apparaitre un consensus relatif sur les conditions d'un consentement valable, à savoir qu'il doit être libre, spécifique et informé* » [860].Toutefois, *« elle met également en évidence un certain flou quant aux manières dont le consentement peut être exprimé : doit-il être explicite, écrit, etc.* » [861]. Cependant, avant de détailler ces différents éléments, il nous faut rappeler que le consentement, est soumis au respect des conditions fixées dans les articles 1128 et suivants du code civil.

533. L'article 1128 énonce que la personne doit posséder la capacité juridique de contracter, délimitant de fait l'usage du consentement comme méthode de légitimation d'un traitement de données à caractère personnel. Cette limitation exclut deux cas de figures. Selon l'article 1146 du code civil : « *sont incapables de contracter, dans la mesure définie par la loi, les mineurs non émancipés ; les majeurs protégés au sens de l'article 425* ». Sans être pris en compte dans la directive, ces deux éléments d'ordre généraux viennent pourtant limiter de facto la capacité d'un responsable de traitement à collecter des données.

534. Concernant les mineurs, il n'existe aucune mention directe de la place du mineur dans le régime applicable aux données à caractère personnel. En l'absence de dispositions particulières, on pourrait considérer qu'un mineur ne puisse pas autoriser un responsable de traitement à collecter ses données, ni même à s'inscrire sur un service en ligne tel que Facebook. Toutefois, selon l'avis du G29, rappelant l'article 6 de la Convention 192 du Conseil de l'Europe, l'article 3 de la Convention des Nations Unies relative aux droits de l'enfant, ainsi que l'article 24 paragraphe 2 de la Charte des droits fondamentaux de l'Union Européenne, « *le principe juridique de base est celui de l'intérêt supérieur de l'enfant* » [862]. Selon le rapport, « *dans la mesure où l'enfant est une personne en développement, l'exercice de ses droits, y compris ceux relatifs à la protection des données, doit être adapté à son niveau de développement physique et psychologique. Non seulement les enfants sont en*

circulation de ces données, Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, article 2.

860 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 6.

861 Ibid.

862 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*, adopté le 11 février 2009, 398/09/FR, WP 160, p. 4.

développement, mais ils ont le droit à ce développement » [863]. L'avis reconnait donc implicitement la validité juridique du consentement du mineur dans le cadre applicable aux données à caractère personnel, pour autant que la procédure soit adaptée.

535. En conséquence, le responsable de traitement devra prendre des mesures relatives à la présentation générales des informations, sur les finalités et les modalités envisagées du traitement, en fonction de l'âge de la personne, afin que ces dernières puissent « *participer plus régulièrement à l'exercice de leurs droits, y compris ceux relatifs à la protection des données* » [864]. Dans sa communication datée du 2 septembre 2015, la CNIL ira dans le même sens, rappelant les « *précautions à pren*dre » lors de la collecte de données en provenance des enfants[865]. Celles-ci relèvent principalement de l'utilisation d'informations intelligibles pour un jeune public, de mesures de contrôle de l'âge ainsi que de la mise en place de modalités d'exercice du contrôle parental. Cette publication fait écho à une étude sur l'insuffisance de la protection des sites internet vis-à-vis de la vie privée des enfants, pilotée par les CNILs Européenne, mettant en avant la tendance au manque d'information et à la collecte large de données personnelles qui étaient effectuées sur ce public, et dont la CNIL prend acte afin d'informer les différents acteurs et prendre des sanctions si nécessaire[866]. Toutefois, on peut remarquer que l'autorité indépendante ne remet pas en cause la licéité d'un traitement de valorisation de données d'une personne mineure, et ne propose aucune différence dans la prise en compte de ce consentement selon l'âge du mineur.

536. Cette doctrine évoluera prochainement, avec la mise en œuvre du nouveau règlement Européen portant sur les données à caractère personnel, dont l'article 8 vise spécifiquement les enfants dans leur rapport au régime de protection[867]. Ainsi, selon le premier alinéa, l'enfant devra être âgé d'au minimum 16 ans pour consentir à un traitement. Dans le cas contraire, le consentement sera « *donnée ou autorisé par le titulaire de la responsabilité*

863 Ibid, p4.
864 Ibid, p4.
865 Commission Nationale de l'Informatique et des Libertés, *Editeurs de sites pour enfants : n'oubliez pas vos obligations*, 2 septembre 2015.
866 Commission Nationale de l'Informatique et des Libertés, *Vie privée des enfants : une protection insuffisante sur les sites internet*, 2 septembre 2015.
867 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

parentale à l'égard de l'enfant » [868]. Le règlement va plus loin, en autorisant les Etats à autoriser le recours à ce consentement pour un enfant d'un âge inférieur, « *pour autant que cet âge inférieur ne soit pas en dessous de 13 ans* »[869]. On retrouve ainsi la logique qui s'applique au majeur protégé de l'article 425 et suivant du Code Civil dans le cadre de certains actes de la vie courante.

537. Toutefois pour ce dernier, aucune mesure dans le nouveau règlement ne vient pallier l'absence d'indications concrètes quant aux modalités applicables au recueil du consentement pour un adulte protégé. Dans ce cas, il faudra se référer aux principes spécifiques liés à la qualité du consentement, et en particulier aux conditions dans lesquelles la volonté s'est exprimée.

3 – Les conditions spécifiques de licéités du consentement

538. Selon la directive 95/46/CE, le consentement est constitué par « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement* » [870]. Il nous appartient de définir la signification individuelle de ces critères.

a) « Toute manifestation de volonté »

539. En premier lieu, la directive définit le consentement comme « *toute manifestation de volonté* » de la part de la personne concernée, sans recourir aux notions déjà existantes de signature électronique, ou de signature électronique sécurisée, que l'on a pu décrire aux points 166 et suivants de cet ouvrage. Á cet égard, on peut noter un écart avec la proposition initiale de la Commission, dans laquelle il était question de consentement « *explicite*», mention qui

868 Ibid.
869 Ibid.
870 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050, article 2.

fut finalement supprimée et remplacée par « *indubitable* ». Selon le G29, cette suppression s'explique essentiellement par une volonté de souplesse dans l'application de la directive, en évitant l'écueil technologique de s'enchainer à un type d'interaction défini entre un responsable de traitement et la personne concernée[871].

540. Cette définition laisse donc une grande liberté dans son interprétation. Ainsi, si l'on se réfère à la directive 2002/58 portant sur le traitement des données dans le secteur des télécommunications, « *le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site internet* » [872]. Celle-ci va jusqu'à préciser que « *les méthodes retenues pour communiquer des informations, offrir un droit de refus ou solliciter le consentement devraient être les plus conviviales possibles* » [873]. La Commission laisse le champ libre aux responsables de traitement pour la mise en place de cette procédure, dans les conditions techniques qui leurs paraissent les plus appropriées en fonction de l'interaction qu'ils développent avec les personnes concernées.

541. Toutefois, la notion d'acceptation, qui se trouve dans la définition, indique qu'il s'agira nécessairement d'une action positive de la part de la personne concernée. Si l'on peut déplorer la suppression du caractère « *explicite* » du consentement, initialement prévue dans la proposition, la Commission laisse aux CNIL Européennes le soin de juger au cas par cas la licéité de ces procédures « *indubitables* ». En France, la CNIL s'est prononcée sur ce point dans le cas de messages envoyés par des panneaux publicitaires utilisant la technologie Bluetooth pour contacter les Smartphones passant à proximité. En l'espèce, le panneau envoyait une demande de connexion Bluetooth afin d'afficher la publicité sur l'appareil de l'utilisateur. Selon La Commission Nationale, cette procédure « *n'est pas une modalité satisfaisante du recueil du consentement dans la mesure où elle intervient trop tardivement* » [874]. En effet, le fait de passer à proximité du panneau après avoir activé la fonction Bluetooth

871 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 13.

872 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47, considérant 17.

873 Tversky Amos, Kahneman Daniel, *The Framing of Decision and the Psychology of Choice*, Science, New Series, Vol. 211, N° 4481, January 30 1981, p. 453.

874 Commission Nationale de l'Informatique et des Libertés, *Pas de publicité via Bluetooth sans consentement*

ne suffit pas pour déduire un consentement. Pour qu'une telle publicité soit acceptable, la CNIL suggère que la personne intéressée approche son appareil à quelques centimètres d'un endroit défini sur le panneau, action positive qualifiant son consentement d'une façon indubitable. De la même manière, le G29 rappelle que le fait d'appeler un numéro de téléphone pour recevoir des informations météorologiques « *peut être considéré comme la manifestation du consentement à être localisé* », sous réserve que l'individu ait été suffisamment informé en amont[875]. Ainsi, une action physique peut constituer un consentement juridique.

542. Cependant, on peut se poser la question de savoir si l'absence d'exercice d'une action de refus constitue une action positive d'acceptation. Dans son avis 15/2011 portant sur la définition du consentement, le G29 prend l'exemple d'une lettre informant du transfert de leurs données les personnes concernées, dans laquelle serait précisé que celui-ci aura lieu en l'absence d'opposition de leur part sous deux semaines. Dans ce cas, « *il est douteux que les 90% de clients qui n'ont pas répondu soient effectivement d'accord avec le transfert. En pareils cas, le responsable du traitement n'obtient pas de manifestation claire de la volonté des personnes concernées. En outre, il n'aura pas de preuve et sera donc dans l'incapacité de démontrer qu'il a obtenu un consentement* » [876]. Selon cette approche, l'absence d'action ne peut pas constituer un consentement.

543. Pourtant, on peut opposer à ce raisonnement ce qui est aujourd'hui utilisé pour recueillir le consentement de l'internaute à la collecte de ses informations par l'intermédiaire des cookies. Visé par la directive 2002/58/CE[877] et la directive 2009/136/CE[878], ce type de

---

préalable, Communication du 12 novembre 2008.

875 Groupe de Travail « Article 29 » sur la protection des données, *Avis 5/2005 du groupe 29 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée*, adopté le 25 novembre 2005, 2130/05/FR, WP 115, p. 6.

876 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 13.

877 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

878 Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009, *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal Officiel de l'Union

traitements relève du régime de protection des données à caractère personnel et nécessite le consentement préalable de l'internaute avant le dépôt sur son terminal de cette technologie de collecte d'informations numérique. Or, selon la recommandation de la CNIL en date du 16 décembre 2013, «*le site visité doit comporter un bandeau informant l'internaute que la poursuite de sa navigation vaut accord pour l'installation et la lecture de cookies. Ce bandeau doit mentionner les finalités des cookies utilisés et informer de la possibilité de s'y opposer (via un lien vers une page dédiée du site). Ce bandeau ne doit pas disparaitre tant que l'internaute n'a pas poursuivi sa navigation* » [879]. La CNIL va considérer que c'est l'absence de notification contraire, associée au fait pour l'internaute de continuer sa navigation sur le site internet qui va qualifier le consentement au traitement de ses données. Cependant, il est possible de remettre en cause la qualification d'action positive de la continuation de la navigation, puisque l'utilisateur ne change pas son action initiale consistant à consulter le site internet.

544. Dès lors, on peut considérer qu'il existe une limite extrêmement fine entre l'impossibilité de qualifier un consentement par une absence d'action positive et le raisonnement de la CNIL qui le qualifie en l'associant à l'affichage d'un bandeau d'information. Toute continuation d'une action de la part de l'utilisateur qualifie-t-elle un consentement à partir de l'instant ou une information a été disponible ? Le fait de marcher dans les couloirs du métro est-il un consentement indubitable à partir de l'instant ou un panneau d'affichage a indiqué l'enregistrement et l'exploitation des données issues de la vidéosurveillance pour des finalités mercantiles ? Afin de répondre à ces questions, il faut se pencher sur l'exigence d'information préalable.

Européenne n°L337/11, 18 décembre 2009.

879 Commission Nationale de l'Informatique et des Libertés, « *Recommandation sur les cookies : quelles obligations pour les responsables de sites, quels conseils pour les internautes ?* », 16 décembre 2013.

b) «[…] Informée… »

545. La manière dont on informe une personne est déterminante en termes d'impact sur la vie privée, d'une part parce que c'est à partir de cette procédure que le responsable de traitement obtiendra l'autorisation de traiter les données, d'autre part parce que la présentation des informations est un facteur de décision en soit. De fait, si l'on peut discuter de la pertinence de l'application de la théorie de l'autonomie de la volonté ou de la théorie du solidarisme contractuel, nous sommes contraints de reconnaitre l'influence qu'exerce la présentation des informations au moment du choix, ainsi que la façon dont on qualifie le degré d'information suffisant pour effectuer un choix éclairé. Selon Amos Tversky et Daniel Kahneman : « *la définition de la rationalité a été particulièrement débattue, mais il y a un consensus général sur le fait que les choix rationnels doivent satisfaire des conditions de constances et de cohérence […]. De même, les choix rationnels requièrent que cette préférence ne s'inverse pas en fonction de la manière dont ils sont affichés. Pourtant, à cause des imperfections de la perception humaine des mécanismes de décisions, le changement de perspective implique souvent une inversion de la taille apparente des objets ou de leur désirabilité* »[880]. On peut donc penser que cette liberté pourrait être détournée par les responsables de traitement afin d'obtenir plus facilement un consentement.

546. Pour pallier ce risque, la directive met en place une obligation d'information qui va servir de support au consentement. De manière concrète, on peut effectuer un parallèle avec l'exigence d'information qui existe dans le régime applicable aux données médicales. Pour celles-ci, le G29 considère « *qu'un consentement […] doit être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action. La personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents, en particulier ceux spécifiés aux articles 10 et 11 de la directive, tels que la nature des données traitées, les finalités du traitement, les destinataires d'éventuels*

880 Traduction par l'auteur de: « *the definition of rationality has been much debated, but there is general agreement that rational choices should satisfy some elementary requirements of consistency and coherence. […] Similarly, rational choice requires that the preference between options should not reverse with changes of frame. Because of imperfections of human perception and decision, however, changes of perspective often reverse the relative apparent size of objects and the relative desirability of option* ». Tversky Amos, Kahneman Daniel, *The Framing of Decision and the Psychology of Choice*, Science, New Series, Vol. 211, N° 4481, January 30 1981, p. 453.

transferts et ses droits. Cela suppose également la connaissance des conséquences du refus de consentir au traitement des données en question »[881]. Toutefois, il faudra s'assurer de la satisfaction de deux critères supplémentaires pour que fourniture d'informations puisse être valide.

547. Il s'agira d'abord de vérifier la qualité des informations que le responsable de traitement aura mises en possession de la personne concernée, afin que celle-ci soit en mesure d'évaluer les impacts du traitement. Ensuite, il faut que l'information soit visible et accessible. En prenant appui sur l'arrêt de la Cour Européenne en date du 5 octobre 2004 qui s'attachait à définir la forme que doit prendre cette information dans un contrat de travail, les conditions d'information suffisantes « *ne sont pas remplies des lors que le contrat de travail de l'intéressé se borne à faire référence à une convention collective qui autorise un dépassement de la durée maximale hebdomadaire de travail. En effet, il n'est nullement certain que, lorsqu'il a conclu un tel contrat, le travailleur concerné avait connaissance de la restriction apportée aux droits que la directive 93/104 lui confère* » [882]. Si l'on applique cette logique au régime protecteur des données à caractère personnel, l'ensemble des informations relatives au traitement doit être exposé, et un simple renvoi ne saurait être suffisant. Selon le G29 « *les informations doivent être visibles (type et taille de la police de caractères), mises en évidence et complètes. Des boites de dialogue peuvent être utilisées pour fournir des informations spécifiques au moment où le consentement est demandé* » [883].

548. Toutefois, à ce stade, on peut une nouvelle fois noter qu'il existe une contradiction dans le régime applicable aux cookies que l'on a décrit précédemment. Dans celui-ci, le bandeau d'information ne fait figurer que les modalités d'acceptation de la collecte, ainsi qu'un simple lien vers les conditions détaillées de la collecte et de la mise en œuvre du traitement. En pratique, il est donc difficile de savoir si l'information suffisante est caractérisée par une information sur les modalités de consentement au traitement à partir d'un

881 Groupe de Travail « Article 29 » sur la protection des données, *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, adopté le 15 février 2007, 00323/07/FR, WP 131, p. 11.

882 CJCE, gr. ch., 5 octobre 2004, *X. c. Deutsches Rotes Kreuz*, aff . C-397/01 à C-403/01, point 85.

883 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 22.

comportement défini, ou bien s'il s'agit, comme dans le cas d'espèce relevé par la décision du 5 octobre 2004[884], d'une irrégularité pour défaut d'information complète sur le traitement.

549. Enfin, on peut remarquer que cette solution se distingue de ce qui a été mis en place dans le cadre du droit de la consommation pour les internautes. La directive 2011/83 avait imposé l'utilisation d'un « *support durable* » pour que les informations liées aux conditions générales de vente puissent être conservées par un utilisateur[885]. Celui-ci, à la lumière de la jurisprudence Européenne ne peut être un lien hypertexte seul, mais doit être nécessairement accompagné d'un lien permettant le téléchargement des conditions générales de vente. Le recours à une terminologie similaire aurait sans doute évité la difficulté d'évaluer le niveau suffisant d'information avant le consentement. Toutefois, un autre critère vient renforcer la protection : celui de la spécificité de la manifestation de la volonté.

c) « Spécifique »

550. Lié à l'obligation d'information, le caractère spécifique du consentement vient renforcer l'idée que la personne est en mesure de faire un véritable choix en amont du traitement, et de signifier son accord à celui-ci jusque dans ses moindres détails. Selon le G29 : « *Pour être spécifique, le consentement doit être intelligible. Il doit mentionner, de façon claire et précise, l'étendue et les conséquences du traitement des données. Il ne peut pas s'appliquer à un ensemble illimité d'activités de traitement. En d'autres termes, le contexte dans lequel le consentement s'applique est limité* »[886]. Cela peut prendre la forme de boites de dialogues différenciées qui demandent des autorisations d'accès aux données de manière spécifique à l'instar de ce qu'a créé Facebook avec son API. En l'espèce, lorsqu'une application tierce a recours à l'API de Facebook pour authentifier un utilisateur, une série d'information apparait sur le terminal de l'utilisateur demandant l'autorisation d'accéder à ses données, chacune étant focalisée sur un type de données. En théorie, l'utilisateur pourra donc

884 CJCE, gr. ch., 5 octobre 2004, *X. c. Deutsches Rotes Kreuz*, aff . C-397/01 à C-403/01.

885 Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011, *relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil*, Journal Officiel de l'Union Européenne n°L304, 22 novembre 2011, pp. 64–88.

886 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 19.

effectuer un véritable choix dans la collecte de ses informations, en donnant spécifiquement une autorisation pour chacune des données recueillies.

551. Toutefois, selon l'arrêt de la Cour de Justice de l'Union Européenne en date du 5 mai 2011[887], le consentement initial peut servir à légitimer des traitements futurs. En l'espèce, la société Deutsche Telekom exploitante du réseau téléphonique attribuait des numéros de téléphones à ses abonnés et revendait ces informations à des sociétés tierces à des fins d'éditions de service de renseignements téléphoniques. Ces informations furent publiées par la suite, et mises à disposition du public. L'opérateur avait recueilli préalablement le consentement de l'abonné pour effectuer une telle opération de publication, mais il n'y avait aucune procédure pour renouveler ce consentement dans le cas des entreprises tierces. Or, celles-ci effectuaient bien un traitement de données à caractère personnel au sens de la directive, sans avoir obtenu l'assentiment de la personne concernée. Au regard de l'obligation de spécificité de la définition du consentement, un tel traitement pourrait être considéré comme illicite. Toutefois, la Cour va considérer que « *dès lors qu'un abonné a consenti à la transmission des données à caractère personnel le concernant à une entreprise déterminée en vue de leur publication dans un annuaire public de cette entreprise, la transmission de ces mêmes donnée à une autre entreprise visant à publier un annuaire public, sans qu'un nouveau consentement ait été donné par cet abonné ne saurait porter atteinte à la substance même du droit à la protection des données à caractère personnel, tel que reconnu à l'article 8 de charte* » [888].

552. Par conséquent, l'exigence de spécificité ne s'applique pas au traitement, mais à la finalité déterminée de celui-ci. Selon cette approche, la Cour Européenne semble limiter la portée de cette exigence, en autorisant la création de traitements de seconde main qui auraient les mêmes finalités qu'un traitement initialement autorisé. En France, la CNIL propose une approche similaire. Dans sa délibération du 1 juin 2015, la Commission Nationale de l'Informatique et des libertés se penche sur une société qui « *permet à un internaute de demander à recevoir, par voie de formulaire, la lettre d'information du titre du site qu'il consulte mais également celles des autres revues ou périodiques édités par la société en*

887 CJUE gr. ch., 5 mai 2011, *Deutsche Telekom AG c/ Bundesrepublik Deutschland*, aff. C-543/09.
888 Ibid. Point 66.

cochant une case : oui, je souhaite recevoir les newsletters du groupe » [889]. En l'espèce, « *le fait de cocher la case susmentionnée entraine la réception de lettres d'information destinées notamment à promouvoir d'autres titres de la société ainsi que des biens ou services proposés par des tiers* » [890]. La formation restreinte va considérer que « *la société aurait dû informer l'internaute sur le formulaire de l'intégralité des lettres d'informations auxquelles il consent à s'inscrire* » [891]. Dans ce cas, ce n'est pas la spécificité du consentement qui est en cause, mais l'information préalable qui s'avère insuffisante.

553. Le Conseil d'Etat s'est exprimé dans un cas similaire. En l'espèce, la société proposait un logiciel gratuit dont l'installation entrainait la modification du moteur de recherche par défaut de l'utilisateur et l'envoi de publicités récurrentes grâce à la collecte de données qu'elle effectuait et qu'elle partageait ensuite avec des entreprises tierces. L'installation était soumise à l'acceptation des conditions générales de fonctionnement du logiciel, qui donnait une autorisation générale de traiter les données. Or, selon le Conseil d'Etat qui confirme la décision de la CNIL « *le consentement spécifique […] ne peut résulter que du consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait de ses données personnelles ; qu'alors même que, comme le soutient la société, l'information serait suffisante et les conditions générales d'utilisation claires et explicites, le consentement donné à ces dernières pour l'ensemble des finalités d'un traitement, dont l'usage des données personnelles de l'utilisateur, ne saurait être regardé comme valant consentement spécifique* » [892]. Il appartenait donc à la société de détailler la finalité des différents traitements. Le fait que les données soient ensuite réutilisées par d'autres sociétés ne constitue pas un point d'achoppement.

554. L'exigence de spécificité du consentement s'apprécie en fonction du niveau de détail exprimé par les finalités du traitement. Si celles-ci sont suffisamment définies, le consentement pourra porter sur un nombre presque illimité de traitements ultérieurs. Cette conception est d'autant plus problématique qu'en réduisant cette portée, on touche la liberté dont un utilisateur dispose au moment de consentir.

889 Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2015-155 du 1 juin 2015 *prononçant une sanction pécuniaire à l'encontre de la société X*. Publication non datée.
890 Ibid.
891 Ibid.
892 CE, 11 mars 2015, *TUTO4PC*, n°368624, Mentionné dans les tables du Recueil Lebon, ECLI : FR : CESSR : 2015 :36862.20150311.

d) « libre »

555. Selon le G29, « *le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement. Si les conséquence du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre* » [893]. Afin de savoir si les conditions de libertés suffisantes sont réunies, la CNIL propose d'identifier deux facteurs : « *vérifier qu'il existe une alternative qui ne soit pas trop contraignante (un choix doit être possible) et qu'il n'y a pas de lien de subordination (par exemple entre un employé et son employeur)* » [894]. Pour illustrer ce critère, le G29 prend l'exemple des scanners corporels qui sont placés dans les aéroports à des fins de sécurité. Ainsi: « *le refus de passer dans un scanner corporel pourrait éveiller les soupçons ou provoquer des contrôles supplémentaires, comme une fouille corporelle. De nombreux passagers consentiront à passer dans un scanner afin d'éviter tout problème ou retard potentiel, leur priorité étant de monter à bord de leur avion à temps* » [895]. Ce critère prend en compte l'ensemble du contexte externe à la prise de décision, notamment sur les aspects coercitifs qui pourraient accompagner un refus de consentir.

556. Toutefois, il existe de nombreuses structures dans lesquelles la liberté de consentir peut être remise en question, notamment dans le cadre professionnel et médical. Afin de pallier cette difficulté, le G29 a défini dans plusieurs documents de travail une approche cohérente de la protection dans ces milieux particuliers. Ainsi, dans le contexte professionnel : « *si le consentement du travailleur est nécessaire et que l'absence de consentement peut entrainer un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement […] Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement* » [896].

893 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 14.

894 Commission Nationale de l'Informatique et des Libertés, *Guide : mesures pour traiter les risques sur les libertés et la vie privée*, Edition 2012, p. 11.

895 Avis 15/2011 sur la définition du consentement, Op Cit, p. 17.

896 Groupe de Travail « Article 29 » sur la protection des données, *Avis 8/2001 sur le traitement des données à*

Toutefois, le document souligne que « *aussi longtemps qu'ils font partie d'une organisation, les travailleurs doivent accepter un certain degré d'intrusion dans leur vie privée et doivent partager certaines informations personnelles avec leur employeur. Ce dernier a un intérêt légitime à traiter des données à caractère personnel relatives à ses travailleurs pour des raisons légales et légitimes, nécessaires au développement normal de la relation professionnelle et au bon fonctionnement de l'entreprise* » [897]. En conséquence, il existe bien une légitimité dans le fait de recueillir des données sur le personnel, mais cela doit être fait avec le consentement de la personne de manière à ce qu'il puisse « *se dégager de son consentement sans préjudice* » [898].

557. La même approche est prônée en ce qui concerne l'environnement médical. Ainsi, « *un consentement donné sous la menace de privation de traitement ou de traitement de moindre qualité dans une situation médicale ne saurait être considéré comme libre […]. Lorsque la situation médicale exige nécessairement et inévitablement que le praticien de la santé traite des données à caractère personnel dans un système DME, il est trompeur que ce praticien cherche à légitimer ce traitement par le consentement. Le recours au consentement doit être limité aux cas ou la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice* » [899]. Encore une fois, c'est la double présence d'une absence d'élément coercitif et de possibilité de retirer son consentement ultérieurement qui va qualifier la liberté de consentir.

558. Ces différentes conditions sont toutefois à mettre en parallèle avec les notions connexes de la licéité du consentement.

---

caractère personnel dans le contexte professionnel, adopté le 13 septembre 2001, 5062/01/FR, WP48, p. 31.

897 Ibid. p24.

898 Ibid. p31.

899 Groupe de Travail « Article 29 » sur la protection des données, *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, adopté le 15 février 2007, 00323/07/FR, WP 131, p. 9.

4 – Les notions connexes de la licéité du consentement

559. Il existe trois notions régulièrement mises en avant par les analystes du régime. Il s'agit des notions de contrôle, de transparence, et de temporalité de don du consentement. Mais si elles sont invoquées presque systématiquement lors des débats entourant le régime de protection des données à caractère personnel, il n'y a que peu de traces matérielles de leur existence dans les textes. Il convient donc de déconstruire ces notions avant d'en rechercher les fondements.

560. En premier lieu, le contrôle traduit l'idée selon laquelle le consentement de la personne est susceptible de changer dans le temps et que celui-ci garde la possibilité de décider à tout moment de l'utilisation qui est faite de ses données. C'est d'ailleurs l'un des argument principaux du nouveau règlement européen sur les données à caractère personnel, que selon le communiqué en date du 1 juin 2016 : « *le règlement remplace la directive sur la protection des données de l'UE, qui date de 1995 alors qu'internet était encore à ses débuts, et convertit le patchwork actuel des législations nationales en un ensemble unique de règles en vue de donner aux citoyens plus de contrôle sur leurs propres informations privées dans un monde numérique de téléphones intelligents, de médias sociaux, de services bancaires sur internet et de transferts mondiaux* » [900]. Selon les principaux partisans du texte, le renforcement de la définition des conditions applicables au consentement va donner une plus grande liberté aux utilisateurs dans leur façon de partager, ou non, des données. Si la notion est bien présente dans les considérants du texte, il n'en ai fait aucune mention dans ses articles relatifs au consentement de la personne.

561. À l'inverse, la notion de transparence bénéficie d'une véritable reconnaissance. Celle-ci s'approche de l'obligation d'information qui existait déjà dans la directive, mais dont la mention expresse était quasiment absente des textes[901]. Selon le G29, « *la transparence ne suffit pas, en soi, pour légitimer un traitement de données à caractère personnel, mais elle est*

900 Site d'information du Parlement Européen, Q&R : Les nouvelles règles de l'UE sur la protection des données placent les citoyens aux commandes, droits fondamentaux, 1 juin 2016, disponible sur http://www.europarl.europa.eu/news/fr/news-room/20160413BKG22980/nouvelle-l%C3%A9gislation-europ%C3%A9enne-sur-la-protection-des-donn%C3%A9es (consulté le 01/02/16).

901 À l'exception de sa présence dans le considérant 63 de la directive 95/46/CE.

une condition essentielle pour garantir que le consentement est valable. […] indépendamment du fait que le consentement soit accordé ou non, la transparence du traitement des données est également une condition de loyauté, qui a une valeur propre même après la fourniture de l'information initiale » [902]. Grâce au nouveau règlement, celle-ci intègre les articles 12 et suivants, en devenant l'un des critères de qualification de l'obligation d'information. Ainsi, « *le responsable du traitement prend des mesures appropriées pour fournir toute information […] ainsi que pour procéder à toute communication […] en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant* ». La notion vient ici renforcer l'obligation d'information qui existait à l'article 10 de la directive 95/46/CE qui ne faisait que lister les éléments à fournir obligatoirement à la personne concernée.

562. Enfin, la question de la temporalité du don du consentement, dont la directive 95/46/CE n'avait pas précisé les conditions de recueil, laisse moins de place à l'interprétation. Selon le G29 «*L'importance du fait que le consentement soit un acte positif exclut de facto tout système par lequel la personne concernée n'aurait le droit de s'opposera au transfert qu'après qu'il a eu lieu* » [903]. Il s'agira donc nécessairement d'un consentement donné a priori, dont la formulation passée : « *a indubitablement donné son consentement* » [904] consacre le caractère liminaire. Cependant, il ne s'agit là que d'une modification cosmétique reprenant le terme « *indubitable* » déjà présent dans la directive 95/46/CE.

902 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 10.

903 Groupe de Travail « Article 29 » sur la protection des données, *Document de travail relatif à l'interprétation commune des dispositions de l'article 29, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995*, adopté le 25 novembre 2005, 2093-01/05/FR, WP114.

904 Directive 95/46/CE, Article 7, Op Cit.

Conclusion

563. La notion de consentement est d'une grande importance, de par sa complexité et son développement jurisprudentiel. Si l'on peut en résumer les différentes approches, le consentement apparait comme la somme d'une reconnaissance de l'existence d'une volonté chez un individu, et du choix de s'engager qui en découle. De ces deux éléments, il appartient à la jurisprudence de déterminer celui qui prime sur l'autre pour constituer la partie majeure du consentement. À cet égard, les partisans du solidarisme contractuel font primer la volonté initiale qui a motivé l'engagement, et affrontent l'école libérale de l'autonomie de la volonté qui privilégie l'obligation consentie. Dans ce contexte, les éléments définissants les conditions de licéité du consentement dans le régime applicable aux données à caractère personnel prennent une grande importance liée à la philosophie qui accompagne le régime.

564. En l'espèce, on remarque que les conditions générales et spécifiques de licéité définissent une manifestation de volonté libre, spécifique et informée. Il apparait toutefois, à travers l'étude de ces notions, qu'il s'agit davantage de conditions formalistes que d'une véritable protection de la volonté initiale de la personne. A titre d'exemple, on peut se référer à la décision de la CNIL en date du 15 décembre 2016 qui reprend les différentes conditions que nous avons évoqué dans ce titre. Dans cette affaire, un opérateur de site de rencontre ne donnait qu'une seule case à cocher lors de l'inscription, qui signifiait à la fois l'acceptation des conditions générales de services, les conditions de majorités et l'autorisation de traitement des données sensibles. En défense, la société « *fait principalement valoir que le consentement recueilli est parfaitement informé et qu'il répond à la définition Européenne et Française d'un consentement spécifique ; qu'en tant que tel, le consentement recueilli doit être considéré comme exprès et qu'il satisfait aux conditions de l'article 8 de la loi du 6 janvier 1978 modifié* » [905]. Le consentement est donc, d'après elle, parfaitement libre, spécifique et informé. Cependant, la formation restreinte va considérer « *qu'en recueillant le consentement des personnes par le biais d'une seule et unique case à cocher relative à trois informations distinctes (la majorité, l'acceptation des CGU et l'acceptation du traitement des données relatives à l'orientation sexuelles) diluant ainsi l'information portant sur les données*

905 Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.

relatives à l'orientation sexuelle parmi d'autres, la société n'a pas recueilli le consentement exprès des utilisateurs du site internet de la société au traitement de leurs données sensibles » [906]. Pour que ce traitement soit licite, il fallait mettre en place une case dédiée.

565. Ce jugement résume à lui seul les différentes conditions de licéité du consentement que nous avons évoqué précédemment, appliquées avec rigueur par la CNIL. Pourtant, l'un des arguments de la défense retient particulièrement l'attention. La société « *précise également que les utilisateurs ne seraient pas mieux protégés ni plus libres en souscrivant à l'ensemble des conditions (majorité, acceptation des CGU et traitement des données sensibles) en trois fois plutôt qu'une* » [907]. Pour comprendre la mesure de cette remise en cause implicite de la capacité de protection du régime, il faut nous pencher sur la valeur réelle du consentement dans ce type de traitement.

Section 2

La valeur du consentement dans la valorisation des données à caractère personnel

566. Le régime de protection a mis en place un certain nombre de droits pour la personne concernée ainsi que des conditions strictes encadrant l'exploitation des données à caractère personnel. Toutefois, comme nous l'avons exposé, le consentement est devenu progressivement l'élément principal de la licéité des traitements, tant son recours s'est généralisé grâce aux conditions générales de services. Mais à partir de ce dernier, le responsable de traitement est en mesure de lever une grande partie des restrictions d'usages de données, notamment concernant les données sensibles, et de s'octroyer une grande latitude dans les finalités et l'exploitation qu'il entend tirer de celles-ci. Devenues omniprésentes, ces conditions générales de service autorisent aujourd'hui des collectes et des méthodes de valorisation intensives qui semblent entrer en contradiction avec l'esprit des textes.

906 Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.
907 Ibid.

567. L'ensemble de cette structure, juridique et économique, tourne autour d'un seul axe : celui du respect de l'expression de la volonté de la personne concernée. Erigé comme étendard de la protection des citoyens Européens, le consentement est présenté par les législateurs Européens comme un instrument de contrôle supérieur à tout autre mécanisme de protection, mettant en avant l'image d'un utilisateur puissamment armé face aux velléités des responsables de traitements peu scrupuleux[908].

568. Toutefois, le constat que nous faisons de l'utilisation extensive des données collectées amène à questionner ce raisonnement. Compte tenu de l'écart flagrant qui existe entre la communication sur les prétendues vertus de la structure du régime centrée sur le consentement, et son utilisation concrète, la question de la valeur du consentement dans le régime applicable aux données à caractère personnel s'impose. Si le consentement reproduit avec une grande fidélité la volonté de la personne, nous pouvons conclure que le régime est efficace. Cependant, s'il existe un écart important entre les souhaits de la personne concernée et ce à quoi elle a consentit, la structure de protection apparait d'avantage comme un instrument de légitimation des traitements qu'un facteur d'expression de la volonté de la personne. Dans cette seconde conception, le consentement serait alors un instrument de subordination du citoyen aux objectifs de valorisation des GAFA.

569. Après avoir défini les éléments qui fondent la licéité du consentement dans le régime applicable aux données à caractère personnel, il nous appartient de vérifier leur efficacité pour assurer à la personne concernée une véritable protection.

1 – Une manifestation de la volonté opportuniste

570. Il est possible de considérer que lors de son inscription, un utilisateur souhaite bénéficier d'un service sans pour autant consentir à la monétisation de ses données. Or, en prenant comme référence le comportement de la personne concernée pour interpréter le

908 «*The new EU Laws are designed to put you in control of your own information and safeguards your right to personal data protection* ». Commission Européenne, Directorate General for Justice, *Take control of your personal data*, Luxembourg, Publications Office of the European Union, 2012, p. 3.

consentement explicite à l'utilisation de ses données, le législateur assimile la volonté d'accès à celle de l'utilisation des données. Celle-ci est particulièrement évidente lorsque l'on observe les dispositions spécifiques à l'utilisation des publicités comportementales sur internet, basées sur la technologie des cookies.

571. Intégrée dans la plupart des pages internet, la publicité comportementale « *vise à étudier les caractéristiques de ce comportement à travers leurs actions (visites successives de sites, interactions, mots clés, production de contenu en ligne, etc.) pour établir un profil spécifique et proposer aux personnes concernées des publicités adaptées à leurs centres d'intérêt ainsi déduits* »[909]. Ce traitement repose sur un maillage complexe articulé autour des fournisseurs de réseaux publicitaires, diffusant la publicité et servant d'intermédiaire entre des annonceurs désireux de promouvoir un produit et les diffuseurs, propriétaires des sites internet que l'internaute visite et sur lequel s'affichera la publicité. Ce type de collecte est aujourd'hui l'un des plus importants en termes de périmètre de captation, à l'instar du service Google Adsense qui est présent sur plus de 14 millions de sites internet[910]. Comme nous l'avons exposé précédemment, ce type de technologie est encadré par le régime protecteur des données à caractère personnel issue de la directive 95/46/CE[911] ainsi que par la directive 2002/58/CE[912]. En conséquence, il faudra nécessairement le recueil préalable du consentement de la personne pour traiter ses données.

572. Dans son avis 2/2001 sur les publicités comportementales[913], le G29 va livrer son analyse sur les différentes méthodes permettant d'acquérir le consentement de manière licite pour ces technologies. Selon lui, « *les personnes concernées ne sauraient être réputées avoir donné leur consentement simplement parce qu'elles ont acheté/utilisé un navigateur ou une*

909 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale en ligne*, adopté le 22 juin 2010, 00909/10/FR, WP 171, p. 5.

910 Données publiées par BuiltWith, disponible sur https://trends.builtwith.com/websitelist/Google-Adsense (Consulté le 01/02/2017).

911 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

912 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

913 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale en ligne*, adopté le 22 juin 2010, 00909/10/FR, WP 171, p. 15.

autre application qui permet, par défaut, la collecte et le traitement de leurs informations. Les personnes concernées moyennes ne sont pas au courant du traçage de leur comportement de navigation, des finalités de celui-ci, etc. […] Il est donc fallacieux de considérer que, de manière générale, l'absence d'action de la personne concernée (elle n'a pas configuré les paramètres du navigateur pour qu'il refuse les cookies) est une manifestation claire et sans équivoque de sa volonté »[914]. En cela, le G29 confirme sa doctrine liant consentement et acte positif d'engagement de la part de la personne concernée. Toutefois, cela transforme l'obligation de recueillir le consentement en une constatation de comportement de la part de l'internaute. Dans la communication de la CNIL présentant des exemples de bandeau d'information, l'autorité indépendante propose de matérialiser ce consentement en l'acte positif de « *poursuivre la navigation* »[915].

573. Ce faisant, le régime a opéré une translation sémantique en changeant le consentement en manifestation de volonté, puis en un acte positif qui serait défini à l'avance par le responsable de traitement. En l'espèce dans le cas des cookies, la simple navigation sur un site internet vaut acceptation de l'ensemble des traitements qui peuvent être déployés par les plateformes de publicité comportementales.

574. Cela est d'autant plus préoccupant que les données sensibles sont soumises au même type de régime. Pour le G29, « *tout ciblage des personnes concernées sur la base d'informations sensibles ouvrirait la voie à des abus. […] de ce fait, la seule base juridique susceptible de légitimer le traitement de ces données serait le consentement préalable explicite et distinct, prévu à l'article 8 paragraphe 2, point a) […]. Pour collecter et traiter licitement ce type d'information, les fournisseurs de réseaux publicitaires devraient mettre en place des mécanismes leur permettant d'obtenir un consentement préalable exprès, distinct du consentement recueilli pour le traitement des données en général* »[916]. Mais si l'on se

914 Ibid, p. 16.

915 Commission Nationale de l'Informatique et des Libertés, « *Exemple de Bandeau Cookies : comment recueillir valablement le consentement des internautes aux cookies et traceurs de votre site ou application web ?* », 30 décembre 2015, site internet de la CNIL, https://www.cnil.fr/fr/exemple-de-bandeau-cookie (consulté le 01/09/17).

916 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale en ligne*, adopté le 22 juin 2010, 00909/10/FR, WP 171, p. 23.

réfère à la jurisprudence de la CNIL dans l'affaire Meetic[917], un second bandeau s'affichant selon la même procédure suffirait à qualifier ce consentement.

575. La même logique est applicable dans le cas des smart cities et de la biométrie à la volée. Ainsi, en 2013, la RATP a souhaité déployer un dispositif test de paiement par reconnaissance faciale[918]. Le système, avorté depuis[919], s'appuyait sur le réseau de vidéo surveillance existant et un algorithme pour être capable de reconnaitre un usager et lui facturer le transport. Un tel procédé, s'il est autorisé en amont par la CNIL, pourrait utiliser une technique de qualification de consentement similaire. Les objectifs même du système viennent s'opposer à une procédure de don du consentement systématique, par exemple en présentant sa carte sur un portique, puisque l'on cherche à créer une plus grande fluidité dans la gestion des passagers. Dès lors, on peut imager qu'une information similaire à celle définie par la CNIL pour les cookies puisse être déployée en amont des points de contrôles, qui préciserait que le fait de continuer son chemin vaut acceptation du traitement de ses données. Ainsi, selon Nathalie Mallet-Poujol, dans ce cas, « *la biométrique est d'avantage subie et pourra d'ailleurs de plus en plus se faire à l'insu de la personne* »[920]. Après l'autorisation préalable de la CNIL, une demande initiale de titre de transport pourrait suffire à constituer le consentement, renouvelé chaque fois que l'usager souhaitera emprunter les transports en commun.

576. Dans cette configuration, la qualification de la manifestation de la volonté devient opportuniste. En sélectionnant en amont les actions qui vont déterminer le consentement de l'utilisateur au traitement, le responsable de traitement est capable de rendre difficile, voire impossible la capacité d'un individu à refuser le traitement. Au minimum, cela va considérablement réduire la valeur du consentement. Que ce soit dans le cadre de la

917 Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.

918 Next-impact, *Biométrie : la RATP veut faire payer à la face pour supprimer les queues*, Next Impact, 22 mai 2013, disponible sur https://www.nextinpact.com/news/79897-biometrie-ratp-veut-faire-payer-a-face-pour-supprimer-queues.htm (consulté le 01/09/17).

919 Next-impact, *La RATP abandonne son projet de péage par reconnaissance faciale,* Next Impact, 22 mai 2013, article disponible sur https://www.nextinpact.com/news/79901-la-ratp-abandonne-son-projet-peage-par-reconnaissance-faciale.htm (consulté le 01/09/17).

920 Mallet-Poujol Nathalie, propos retranscrits dans Commission Nationale de l'Informatique et des Libertés, *Cahiers IP, Innovation et prospective n°1, Vie privée à l'horizon 2020 : Paroles d'experts,* 30 novembre 2012, p. 55.

consultation d'un site internet ou dans le fait de prendre les transports en commun, on peut critiquer le fait qu'un consentement puisse être déduit du comportement d'utilisation normal. Dans une situation pareille, la personne concernée devra se référer aux informations qui lui auront été données en amont, afin d'éventuellement opposer un refus. Pourtant, on peut douter de la portée réelle de l'obligation d'information.

2 – Une obligation d'information à la portée relative

577. D'après la législation, l'information doit précéder le consentement. Celle-ci doit détailler les modalités du traitement, finalités et périmètre de collecte, mais également les droits et mesures permettant de les exercer. Il est donc possible de scinder cette obligation en deux objectifs, l'un portant sur la compréhension suffisante du traitement envisagé et sur ses conséquences, l'autre sur les modalités d'exercice des droits de la personne.

a) La compréhension de l'impact du traitement : le problème de l'asymétrie informationnelle

578. Sur le premier point, il s'agit des informations visées par l'article 10 de la directive 95/46/CE[921], que l'on a déjà détaillées précédemment. La directive 2002/58/CE précise dans son considérant 25 que les informations relatives aux technologies cookies doivent être communiquées de la façon « *la plus conviviale possible* » [922]. Dans son avis 2/2010, la G29 ajoute que « *la fourniture d'un minimum d'informations directement sur l'écran, de manière interactive, aisément visibles et compréhensibles, serait le meilleur moyen de se conformer à ce principe. Il importe que les informations soient aisément accessibles et extrêmement visibles. Ces informations essentielles ne peuvent donc pas être cachées dans des conditions générales et/ou dans des déclarations sur la politique de confidentialité* » [923]. Si cette

921 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

922 Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

923 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale*

remarque vaut uniquement pour l'obligation d'information relative au consentement préalable à l'utilisation des technologies de publicité comportementale, on peut la comprendre comme un aveu de faiblesse de la procédure générale d'information, qui repose bien souvent sur l'information disponible dans les conditions générales. Cette observation du G29 relève d'un problème que l'on pourrait qualifier d'asymétrie informationnelle. A un double niveau, il existe une inégalité dans la connaissance des informations relatives au traitement des données, à la défaveur de l'utilisateur.

579. Tout d'abord, l'information dont l'utilisateur va disposer sur un traitement est bien inférieure à celle détenue par le responsable de traitement. Au-delà de la simple donnée qu'il va recueillir, le responsable de traitement va développer un ensemble de techniques algorithmiques à des fins de valorisation, pour produire le profil le plus détaillé possible de l'utilisateur. Les données seront agrégées, et deux types de profils peuvent être définis. Ainsi, « *les profils prédictifs sont établis par déduction en observant le comportement individuel et collectif des utilisateurs dans le temps, notamment en suivant les pages visitées et les publicités qu'ils ont vues ou sur lesquelles ils ont cliqué* » [924].

580. Quant aux seconds, « *les profils explicites sont établis à partir des données à caractère personnel que les personnes concernées fournissent elles-mêmes à un service web, notamment par leur inscription* » [925]. Ces deux flux d'informations sont combinés, mais peuvent provenir de différents moyens de collecte, voire même de différents services. À titre d'exemple, Google a récemment fusionné ses conditions générales de service, englobant ainsi des services aussi hétéroclites que Gmail, Google Maps, Youtube et ses services de publicité en ligne. Si des détails ont été précisés depuis la sanction de la CNIL à l'égard de cette évolution[926], et malgré un pack de conformité produit par le G29[927], aucune précision sur la mécanique interne de valorisation des données n'a filtrée. L'utilisateur n'est donc pas en mesure d'évaluer l'impact de la collecte de ses informations par le géant de Mountain View pour des raisons structurelles. Selon Daniel Solove, « *le type de nouvelles d'informations qui*

en ligne, adopté le 22 juin 2010, 00909/10/FR, WP 171, p. 8.

924 Ibid. p. 16.

925 Ibid, p. 16.

926 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

927 Groupe de Travail « Article 29 » sur la protection des données, *Google Privacy Policy*, Ref. Ares (2014) 3113072, 23 septembre 2014.

peuvent être conçues par l'analyse des informations existantes ainsi que celles qui peuvent être prédites est trop vaste, trop complexe, et évoluent trop rapidement pour que les personnes puissent prédirent avec suffisamment de certitudes les risques et les bénéfices impliqués. Cet état de fait rend très difficile l'évaluation de l'impact du don d'une information qui sera parfois, dans le futur, associée à une nouvelle donnée qui révèlera quelque chose de sensible »[928].

581. De la même manière, il est presque impossible pour un utilisateur de savoir quel va être le niveau de partage de ses propres informations avec les partenaires du service auquel il s'est lié initialement. L'obligation d'information force le responsable de traitement à déclarer la finalité de la valorisation des données, ainsi que leur partage avec des entités tiers, mais il n'est pas possible de connaitre exactement lesquelles. Enfin, se pose la question de la durée de l'autorisation de traitement accordée par le consentement. Toujours selon le G29 : « *à moins que des rappels clairs et non équivoques, recourant à des moyens simples, ne soient adressés aux personnes concernées, il est très probable qu'après un certain temps, ces dernières auront oublié que le suivi se poursuit et qu'elles y ont consenti* » [929]. S'il existe des durées fixes de conservation des données cookies, le régime général accorde une autorisation au traitement dans son ensemble et pour la durée nécessaire à la réalisation de ses finalités. Or, l'information d'origine n'est pas forcément disponible quelques années après le début du traitement.

582. Dès lors, il est difficile de considérer que l'obligation d'information, sous sa forme actuelle, remplie pleinement son rôle. D'autant que cette difficulté d'ordre structurelle est complétée par un problème cognitif.

928 Traduction par l'auteur de: « *the type of new information that can be gleaned from analyzing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved. This state of affairs makes it very hard to assess whether revealing any piece of information will sometimes later one, when combined with other data, reveal something sensitive* ». Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, p. 151.

929 Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale en ligne*, adopté le 22 juin 2010, 00909/10/FR, WP 171, p. 12.

b) La compréhension de l'impact du traitement : le problème cognitif

583. Selon Daniel Solove, il existe un problème cognitif dans le fait d'utiliser le consentement comme élément principal de licéité dans le régime protecteur de la vie privée[930]. Celui-ci peut être appréhendé sous deux aspects. Le premier remet en cause le niveau réel de compréhension de la personne concernée dans l'implication de son consentement, le second, plus théorique, pose la question de la capacité d'un individu à prendre une bonne décision pour lui-même dans ce contexte.

584. Sur le premier point, le régime fait état d'un consentement informé, mais n'utilise pas la notion de consentement éclairé, comme c'est le cas en médecine par exemple[931]. Toutefois, le G29 précise que « *la manière dont les informations doivent être fournies dépend du contexte. Un utilisateur régulier/moyen devrait être en mesure de les comprendre* » [932]. En pratique, il est donc difficile de savoir quelle est l'étendue de cette obligation d'information. Est-elle limitée à la fourniture des informations, ou bien implique-t-elle de fournir celles-ci avec suffisamment de détails pour apprécier les impacts du traitement ? Selon la formulation de l'article 12 du règlement Européen sur les données à caractère personnel, l'exigence de transparence oblige le responsable du traitement à prendre « *des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifique à un enfant* ». Cela ne suffira pas à combler le déficit initial que nous avons constaté avec l'asymétrie informationnelle existante, alors même que l'on peut remettre en cause l'efficacité d'une telle information si celle-ci est « *cachée dans des conditions générales et/ou dans des déclarations sur la politique de confidentialité* » [933].

930 v. Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, pp. 14-165 ; Acquisti Alessandro, Grossklags Jens, *What Can Behavioral Economics Teach Us About Privacy?*, Digital Privacy: Theory, Technologies and Practices, Taylor and Francis Group, 2007, pp. 160-179.

931 Cass. Civ. 11 octobre 1988, n°86-12832, Bull. Civ. 1988, n°280, p. 192.

932 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 22.

933 Groupe de travail « article 29 », avis 2/2010, Op Cit. p8.

585. C'est ici le paradoxe de l'information contenue dans les conditions générales de services. Bien qu'elle soit présente, il est peu probable qu'un utilisateur prenne le temps de lire l'ensemble des conditions auxquelles il fait face chaque jour. Nous avions déjà évoqué le temps que prendrait la lecture de celles-ci au point 147 de cet ouvrage, qui rend concrètement impossible la complétion de l'obligation d'information préalable au consentement. La réalité est ici en contradiction avec la théorie juridique. Selon une étude publiée en 2006, seulement 28% des Américains déclarent vérifier « *la plupart du temps* » les règles de confidentialité des services qu'ils utilisent[934].

586. Il faut ajouter à cela la difficulté de connaitre exactement l'impact potentiel du consentement au traitement des données. Du fait de la masse de données collectée à travers le temps, un individu ne peut pas envisager l'ensemble des combinaisons possibles, ou les conclusions tirées de celles-ci dans les prochaines années. Une donnée isolée peut être agrégée dans le futur avec d'autres données issues d'autres entités, et représenter un risque à terme. Ainsi, « *il est virtuellement impossible pour une personne d'effectuer un jugement cohérent à propos des coûts et des bénéfices de révéler une information. Dès lors, dans la plupart des situations, la quantité d'informations manquantes est trop importante pour que la décision de gérer sa vie privée en fonction de ces coûts et bénéfices soit effectuée correctement* »[935]. Ce problème cognitif est en partie résolu par l'intégration au règlement Européen du droit à l'oubli, dans son article 17. Pourtant, d'un point de vue empirique, il est possible de remettre en cause la portée de l'obligation d'information au moment du don du consentement.

587. Cette difficulté dans la compréhension du choix donné à l'utilisateur nous amène au second aspect du problème cognitif qui entoure l'obligation d'information : un individu est-il en mesure de prendre une décision concernant ses données dans le cadre des conditions générales de service ? Selon Alessandro Acquisti et Jens Grossklags: « *même si les personnes avaient accès à une information complète, ils ne pourraient probablement pas traiter une si*

934 Truste/TNS Survey, *Consumers have false sense of security about online privacy, actions inconsistent with attitudes*, Rapport daté du 6 décembre 2006.

935 Traduction par l'auteur de: « *it is virtually impossible for a person to make meaningful judgment about the costs and benefits of revealing certain data. Therefore, in many situations, too much is unknown to make a meaningful decision about costs and benefits at the time that people are asked to manage their privacy* ». Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, pp. 141-165.

grande quantité d'informations et agir en fonction de cette réflexion. Spécialement dans le cadre complexe de la ramification des conséquences associées à la protection ou à la divulgation d'informations personnelles, nos barrières rationnelles initiales limitent notre capacité à acquérir, à mémoriser et à traiter l'ensemble de ces données, conduisant à faire reposer notre réflexion sur des modèles psychologiques simplifiés, des stratégies approximatives, et sur l'heuristique »[936]. Les limites des capacités cognitives entraineraient pour l'individu un risque au moment de faire son choix, choix qui ne serait pas basé sur une compréhension optimale mais sur un raisonnement heuristique. D'ailleurs, ce choix serait biaisé dans la plupart des cas. Selon la Commission des Clauses Abusives : « *de nombreux contrats de fourniture de services de réseautage social prévoient des clauses affirmant que les services proposés sont gratuits ; que ces clauses laissent croire à l'utilisateur consommateur ou non-professionnel que le service est dépourvu de toute contrepartie de sa part, alors que, si toute contrepartie monétaire à sa charge est exclue, les données, informations et contenus qu'il dépose, consciemment ou non, à l'occasion de l'utilisation du réseau social, constituent une contrepartie qui s'analyse en une rémunération ou un prix, potentiellement valorisable par le professionnel […] que ces clauses sont de nature à créer un déséquilibre significatif entre les droits et obligation des parties au contrat au détriment du consommateur ou du non-professionnel en ce qu'elles lui laissent croire qu'il ne fournit aucune contrepartie* » [937]. Dans ce cas, on peut penser qu'il existe une difficulté pour l'internaute à obtenir une véritable compréhension du choix qui lui est imposé. Cela est d'autant plus problématique que la liberté de choix pourrait être remise en cause.

936 Traduction par l'auteur de: « *even if individuals had access to complete information, they would often be unable to process and act optimally on large amounts of data. Especially in the presence of complex, ramified consequences associated with the protection or release of personal information, our innate bounded rationality limits our ability to acquire, memorize and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics* ». Acquisti Alessandro, Grossklags Jens, *What Can Behavioral Economics Teach Us About Privacy?*, Digital Privacy: Theory, Technologies and Practices, Taylor and Francis Group, 2007, pp. 160-179.

937 Commission des Clauses Abusives, Recommandation n°14-02, Contrats de fourniture de services de réseaux sociaux, 7 novembre 2016.

3 – Une liberté de consentir illusoire

588. Pour qualifier la valeur du consentement, le régime intègre la notion de liberté. Celle-ci, définie aux points 66 et suivants de cet ouvrage, suppose une analyse in concreto de l'environnement ou de l'état dans lequel la personne se trouve au moment de consentir au traitement[938]. S'il existe une mesure coercitive externe, réelle ou potentielle, venant sanctionner un refus d'acquiescer, la liberté s'en trouve diminuée et le consentement ne peut pas être pris en compte. Selon le G29 : « *c'est le cas, par exemple, lorsque la personne concernée est sous l'influence du responsable du traitement, dans le cadre d'une relation de travail notamment. Dans ce cas, même s'il n'en est pas nécessairement toujours ainsi, la personne concernée peut se trouver dans une situation de dépendance vis-à-vis du responsable du traitement – en raison de la relation ou de circonstances particulières – et peut craindre d'être traitée différemment si elle n'accepte pas le traitement de ses données* » [939]. Or, cet état de dépendance à l'égard du responsable de traitement existe à l'heure où la présence en ligne et l'utilisation des outils numérique est devenue indispensable.

589. A l'heure actuelle, il est pratiquement impossible pour un citoyen d'échapper à la collecte privée de ses données personnelles. Dès les premiers pas sur internet, le moteur de recherche dépose des cookies sur le terminal de l'utilisateur qui le suivront durant toute sa session de navigation. Les différents sites internet qu'il va consulter seront très probablement équipés d'un algorithme de ciblage publicitaire, et l'inscription à un quelconque service nécessitera l'adhésion aux conditions générales de services, ainsi qu'aux règles de confidentialité portant sur l'exploitation des données. Hormis certaines offres basées sur un modèle économique différent[940], la monétisation des données oblige les applications, les services, et les sites internet à collecter et valoriser les informations des internautes. A ce jour, il existe même des sites internet développant des méthodes logicielles permettant d'empêcher l'accès à une information si le terminal de l'internaute refuse le déploiement et l'exploitation

938 « *Elle précise, en outre, que les modalités de recueil du consentement sur les sites de rencontre doivent etre appréciées in concreto* […] ». Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.

939 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 14.

940 A l'instar du moteur de recherche Français Qwant.

des cookies. Ainsi, un site d'actualité tel que les Echos détecte, puis affiche un message empêchant l'accès à ses articles s'il existe un bloqueur de publicité[941].

590. Le refus de ces conditions d'utilisation, ou des modalités de collecte de ses propres données, interdit l'accès à un service donné. Si l'élément coercitif est difficilement quantifiable en termes d'accès au travail, de capacité à se déplacer, ou tout simplement à entretenir des relations sociales, il est possible d'affirmer que l'utilisateur n'est pas libre de refuser la collecte de ses données sans limiter son accès à l'innovation numérique.

591. Cela remet directement en cause le principe de spécificité dans le consentement. Dans son avis 15/2011 portant sur la définition du consentement, le G29 en fait l'un de ses exemples. Ainsi « *l'accès aux services d'un réseau social est souvent subordonné à l'acceptation de différents types de traitement de données à caractère personnel. […] Compte tenu de l'importance qu'ont pris certains réseaux sociaux, certaines catégories d'utilisateurs (comme les adolescents) consentiront à recevoir de la publicité comportementale pour éviter le risque d'être exclus de certaines interactions sociales. Or, l'utilisateur devrait être en mesure de donner un consentement libre et spécifique à la réception de publicités comportementales, indépendamment de son accès au réseau social. Une fenêtre distincte pourrait être utilisée pour proposer cette possibilité à l'utilisateur* » [942]. Il précise à cette occasion : « *dans la pratique, il est fréquent que l'utilisateur ne puisse pas utiliser une application s'il n'accepte pas la transmission de ses données au développeur de l'application à différentes fins, y compris la publicité comportementale et la revente à des tiers. Etant donné que l'application ne peut fonctionner sans qu'il soit nécessaire de transférer des données à son développeur, le groupe de travail recommande de détailler le consentement de l'utilisateur […]* » [943]. Pour le G29, un détail des finalités suffit à constituer la spécificité du consentement, du moment qu'il s'agit de plusieurs boites de dialogues distinctes à accepter.

592. Cette logique, reprise par la CNIL dans la double délibération du 15 décembre 2016 concernant des sites de rencontres, implique pour le responsable de traitement de distinguer le consentement aux conditions générales de services et le consentement aux règles de

941 Voir site internet LesEchos.fr, (consulté le 01/09/2017).
942 Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187, p. 20.
943 Ibid, p. 21.

confidentialité. Pourtant, comme nous l'avions évoqué précédemment en paraphrasant l'une des sociétés défenderesse : « *Les utilisateurs ne seraient pas mieux protégés ni plus libres, en souscrivant à l'ensemble des conditions (majorité, acceptation des CGU et traitement des données sensibles) en trois fois plutôt qu'une* » [944]. De fait, le service n'est pas accessible si une seule de ces cases n'est pas cochée.

593. Il est possible, ainsi, d'affirmer que la liberté dont dispose un utilisateur, est pratiquement nulle au regard du détournement de l'objectif de spécificité du consentement que la jurisprudence semble développer. En considérant la condition de spécificité comme une formalité d'ordre cosmétique, vis-à-vis de la présentation des informations, elle réduit la capacité d'un individu à effectuer un choix devant les traitements qui lui sont proposés, si seule leur acceptation totale autorise l'inscription.

Conclusion

594. Chaque critère définissant la qualité est porteur d'une contradiction entre ses objectifs initiaux et l'analyse jurisprudentielle de son application concrète. Tout d'abord, la définition, en s'appuyant sur la notion de manifestation de volonté, autorise un responsable de traitement à transformer l'usage normal en manifestation de consentement explicite. Le fait de continuer la navigation sur un site internet donné est interprété comme un consentement à l'installation de cookie sur le terminal de l'utilisateur, et à l'exploitation des données qui seront collectées. Validé à la fois par la directive 2002/58 et la jurisprudence de la CNIL, cette interprétation devient une opportunité pour le responsable de traitement, qui diminue considérablement la valeur du consentement de la personne concernée.

595. De même, l'obligation d'information, qui tend à donner à la personne concernée les moyens d'évaluer l'impact du traitement sur sa vie privée, apparait comme une illusion au regard d'une analyse factuelle. Il n'est pas possible, à partir des informations fournies, de déterminer exactement la mesure du traitement, autant dans sa dimension technique que dans

944 « *Elle précise, en outre, que les modalités de recueil du consentement sur les sites de rencontre doivent etre appréciées in concreto* […] ». Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016, p. 4.

les possibilités futures d'agrégation des données. La transparence évoquée par le nouveau règlement ainsi que l'augmentation du niveau minimum d'information ne peut pallier l'asymétrie informationnelle qui résulte de la mécanique interne du traitement et du partage des informations avec les entités tiers, qui est seulement connue du responsable de traitement. Cette structure influence directement la capacité de la personne concernée à évaluer les risques associés au traitement et à prendre une décision cohérente au regard de la complexité des traitements. Ce biais cognitif est même renforcé par la relation qui va unir la personne concernée et le responsable de traitement, dans un service qui s'identifie comme gratuit, alors qu'en réalité, il exige une forte contrepartie avec l'obtention d'un droit de valoriser les données collectées.

596. Enfin, l'idée d'un consentement libre, dans la définition jurisprudentiel du G29, parait illusoire lorsqu'une relation de dépendance est constatée entre les personnes souhaitant profiter de l'innovation numérique et les responsables de traitement. L'exigence de spécificité du consentement, qui aurait pu différencier l'inscription au service et l'acceptation des règles de confidentialité devient, dans la jurisprudence, une obligation de présentation distincte des informations, dont l'application est essentiellement cosmétique. En aucun cas, celle-ci n'exige de la part du responsable de traitement de distinguer les accès et les services en fonction de l'acquiescement particulier de la personne à tel ou tel traitement de données.

597. La problématique se trouve particulièrement bien illustrée dans le cas d'un changement unilatéral des règles de confidentialité. Ainsi, lorsque Google a décidé de fusionner l'ensemble de ses règles de confidentialité en un seul document, lui permettant de d'agréger l'ensemble des données issues de ses différents services le 1er mars 2012, il a été demandé aux internautes de donner leur consentement une seconde fois à ces traitements. Dans ce texte unique, Il est écrit qu'à travers les nouvelles conditions que l'utilisateur autorise le service à collecter et traiter de nombreuses données pour des finalités très variés. Il était précisé qu'en cas de refus, l'utilisateur sera tout simplement dans l'incapacité d'accéder aux différents services.

598. Jugée dangereuse, cette union fut la cible du G29 et de la CNIL qui mirent en place un pack de conformité[945], presque deux ans après les changements. Toutefois, celui-ci ne fait que reprendre les jurisprudences antérieures, en demandant un renforcement de l'information donnée à l'utilisateur et une plus grande spécificité dans le recueil du consentement. En admettant que ces mesures aient été respectées lors du changement de politique de confidentialité, le consentement de l'utilisateur était-il réellement libre, spécifique et informé ? A la lumière de nos observations, nous pourrions raisonnablement en douter. D'une part, l'utilisateur n'a toujours pas les moyens de prendre la mesure des effets potentiels d'un traitement dont il ignore les rouages et les implications à long terme. D'autre part, il ne peut s'agir d'un consentement libre si le refus entraine le bannissement du plus grand pourvoyeur de services informatiques mondial.

599. Par conséquent, on peut considérer que le consentement, dans sa forme actuelle, est porteur d'une double fragilité juridique. D'une part, ses critères ne permettent pas à un utilisateur d'être réellement autonome dans sa capacité décisionnelle, affaiblissant par corollaire la protection qu'offre le régime. D'autre part, il place la sécurité juridique des investissements, voire même de l'écosystème dans son ensemble, à la merci d'un revirement jurisprudentiel dans l'appréciation de ses critères. Pour ces deux raisons, la valeur du consentement peut être remise en cause. Il convient donc d'apprécier les conséquences de cette remise en cause, à la fois sur le plan économique et structurel, mais aussi en analysant les composants juridiques permettant d'atteindre ses objectifs initiaux.

945 Commission Nationale de l'Informatique et des Libertés, *Politique de confidentialité de Google : le G29 propose un pack de conformité*, 25 septembre 2014.

Chapitre 2

Les conséquences d'une remise en cause de la valeur du consentement

*

600. L'innovation technologique ne se résume pas à la simple possibilité de fournir de nouveaux services aux citoyens. Elle est devenue l'un des enjeux économique et social du monde de demain. Selon le rapport France numérique 2012-2020, « *le numérique est un élément essentiel de notre outil industriel et de notre capacité d'innovation. L'économie numérique représente 3,7% de l'emploi en France et contribue à hauteur de 5,2% à notre PIB et à 7,9% de la valeur ajoutée totale du secteur privée. Le numérique représente un tiers des investissements privés en recherche et développement* » [946]. Et si, dans cet écosystème, l'impact de la robotique et de l'électronique n'est pas à négliger, la valorisation des données reste le principal moteur. A tire d'exemple, la valorisation boursière d'IBM, l'une des plus grandes entreprises informatiques du monde, est actuellement d'environ 170 milliards de dollars. Ses concurrents, Oracle et SAP sont respectivement proches de 170 milliards et 100 milliards de dollars de valorisation. Pourtant même cumulés, ces chiffres restent largement en dessous d'un acteur tel qu'Alphabet (la maison mère de Google), qui culmine à 564 milliards. Dans un même ordre de grandeur, Facebook à récemment dépassé les 387 milliards. Face à cela, le leader mondial de la distribution Wal-Mart, avec ses milliers de magasins et ses 2,3 million d'employés[947], n'est qu'à 200 milliards[948].

946 Services du Premier Ministre, *France numérique 2012 -2020, Bilan et Perspectives,* Paris, Novembre 2011, p. 1.

947 Source : Boursorama, cours du 01/09/2017.

948 Site inernet de Wallmart, disponible sur http://corporate.walmart.com/newsroom/company-facts (consulté le 01/09/2017).

601. Ces différences importantes en termes de valorisations boursières s'expliquent tout simplement par la différence de modèles économiques. D'un côté, des entreprises qui se développent grâce à la création de valeur à partir de produits ou de services. De l'autre, des entreprises qui exploitent les données de leurs utilisateurs. Aux vues des écarts de valorisations boursières, on peut penser que pour un organisme de placement financier, ces dernières semblent bien plus intéressantes de par la certitude de pouvoir rentabiliser une grande masse de données, à l'opposé d'une offre de produit ou de service qui peut peiner à trouver sa cible.

602. Or, tout cet écosystème économique repose sur la possibilité de valoriser les données, et donc par corollaire, sur les méthodes de légitimation des traitements, dont le consentement est la principale source de licéité. Si les critères qui le définissent évoluent au niveau juridique, l'atteinte à l'innovation numérique est donc directe. Une telle remise en cause touche non seulement la valeur boursière des entreprises, mais encore l'économie du secteur dans son ensemble ainsi que les emplois qu'elle soutient.

603. En analysant les critères de qualification de la validité du consentement dans le cadre de la valorisation, on peut mettre en évidence un véritable risque juridique pesant sur l'innovation technologique. Si le consentement perd sa valeur, à l'occasion d'un revirement jurisprudentiel portant sur l'interprétation de ces critères constituants, c'est l'ensemble du modèle économique qui est touché. Pour comprendre cela, il faut exposer les conséquences économiques d'une remise en cause de la valeur du consentement et démontrer, ainsi, la fragilité économique de l'innovation numérique (Section 1). Suite à ces constatations, nous évaluerons la possibilité de l'édiction de nouveaux critères, voire d'une refonte des mécanismes de protection de la vie privée dans l'innovation (Section 2).

Section 1

La fragilité économique de l'innovation numérique

604. En ayant recours à une grande part d'interprétation dans la définition des critères de validité du recueil du consentement, le régime devient dépendant de l'interprétation jurisprudentielle Or, une requalification en défaut de consentement implique de lourdes conséquences pour le responsable de traitement, d'autant que l'action en justice peut se fonder sur un plan pénal, civil, ou administratif, offrant ainsi un large spectre d'actions possibles pour un utilisateur lésé.

605. Sur le plan pénal, il n'y a pas de disposition expresse relative au défaut du consentement applicable dans le cadre du régime des données à caractère personnel. Ainsi, l'article 226-16 vise: « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leurs mise en œuvre prévues par loi* », qu'il puni de cinq ans d'emprisonnement et de 300 000 € d'amende. Mais cette formulation générale laisse un doute quant à l'interprétation que l'on peut donner des formalités préalables. S'agit-il des demandes d'autorisations devant la CNIL, ou bien plus largement de tout type de formalités comme le recueil préalable du consentement ? Avec plus de clarté, l'article 226-19 cible ce type d'infraction, mais la limite aux données à caractère personnel qui « *directement ou indirectement, font apparaitre les origines raciales ou ethniques, les opinions religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle ou à l'identité de genre de celles-ci* ». La sanction est de cinq ans d'emprisonnement et de 300 000 € d'amende.

606. Toutefois, même en l'absence de disposition expresse, le juge pénal est capable d'étendre la portée de certains articles liés aux traitements de données. Ainsi, l'article 226-16 offre la possibilité d'une interprétation opportuniste et peut sanctionner l'absence de consentement en tant qu'obligation préalable au traitement. De plus, le juge peut assimiler le

défaut de recueil préalable du consentement à un « *moyen frauduleux, déloyal ou illicite* » de collecter des données personnelles, punit par l'article 226-18 du code pénal. Enfin, dans le cas d'un refus initial de consentir, les dispositions de l'article 226-18-1 réprouvent expressément « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes* », et punissent de cinq ans d'emprisonnement et de 300 000€ d'amende une telle infraction. Enfin, d'autres articles relatifs aux comportements répréhensibles peuvent être employés, notamment les articles 226-19 et suivants, sanctionnant le détournement de finalité ou la divulgation d'information, pour des peines similaires.

607. Néanmoins, cet arsenal législatif est peu utilisé et les contentieux liés au régime applicable aux données à caractère personnel font rarement l'objet de décisions pénales lorsqu'il s'agit d'examiner la validité du consentement de la personne concernée. Cela peut s'expliquer pour deux raisons.

608. Tout d'abord, dans le cadre général de la protection de la vie privée, et selon François Cordier : « *L'efficacité du dispositif civil mis en place par le législateur, les possibilités offertes au juge, notamment en référé, pour sanctionner ou prévenir les atteintes à la vie privée ont naturellement conduit nombre de victimes à préférer la voie civile quand bien même elles auraient eu la possibilité d'agir au pénal* » [949]. Cela s'applique particulièrement dans les cas où la célérité d'une décision en référé peut diminuer la portée du dommage. De plus, l'article 9 du code civil offre une interprétation plus large aux juges du fond pour qualifier les faits, sans risquer de subir un appel quant à l'applicabilité des dispositions pénales. Toutefois, l'existence de la voie civile seule n'explique pas le manque d'attrait de la procédure pénale.

609. La seconde raison de ce délaissement est qu'il existe, en parallèle de la voie civile et pénale, une voie administrative qui capte la plus grande partie des contentieux. En effet, la particularité du régime de protection applicable aux données à caractère personnel est qu'il relève des compétences de la CNIL. Dans la plupart des cas, c'est donc la CNIL qui va être

949 Cordier François, *L'Atteinte à l'Intimité de la Vie Privée en Droit Pénal et les Médias*, Legicom, 4/1999, n°20, 1999, p. 85.

saisie du contentieux, le ramenant au plan administratif plutôt que pénal. A titre d'exemple, lors de l'examen de la fusion des règles de confidentialité des différents services de Google, c'est la CNIL, et non le juge pénal, qui est intervenu, quand bien même il pouvait s'agir, au sens de l'article 226-18-1 du code pénal, d'une collecte illicite.

610. Dans ce cas d'espèce, selon l'analyse de l'autorité indépendante, ce n'est pas le volet pénal qui va s'appliquer, mais bien les dispositions relatives à sa compétence, en faisant directement référence à la directive 95/46/CE, mais également aux dispositions de la loi informatique et libertés. Ainsi : « *le dépôt de cookies ne relevant pas des exceptions prévues aux alinéas 5 à 7 de l'article 32-II [de la directive], des lors qu'il n'est pas préalable à l'expression d'un consentement spécifique de l'utilisateur, lui-même donné postérieurement à la délivrance d'une information claire et complète quant aux finalités et aux moyens de s'opposer à ce dépôt, constitue un manquement aux obligations qui incombent à la société en l'espèce. Dans ces conditions, il est établi que la société ne respecte pas son obligation d'obtenir le consentement de la personne avant d'inscrire des informations dans l'équipement terminal de communication électronique […]* » [950]. Elle s'appuie pour cela sur sa propre interprétation des définitions de la loi informatique et libertés, et la sanction, conforme aux pouvoirs donnés à la Commission par l'article 45 de la loi du 6 janvier 1978 modifiée, atteint le montant maximal de 150 000€, bien en deçà des sanctions pénales.

611. Or, cet exemple est emblématique de la façon dont sont traités les contentieux relatifs à un manquement à l'obligation de recueil préalable de consentement. Dans la grande majorité des cas d'espèces, il ne s'agit pas d'une absence complète de recueil du consentement, mais d'un contentieux sur l'interprétation de la validité de cette procédure. Dans ce cadre, la CNIL apparait comme la mieux placée pour s'autosaisir et apprécier le manquement, limitant de facto la capacité du juge pénal à intervenir à posteriori au nom du principe de non bis in idem. Ainsi, les conséquences d'une remise en cause de la valeur du consentement dans le traitement des données à caractère personnel ne sont pas à chercher dans le volet pénal ou civil des sanctions envisageables, mais bien dans les capacités de sanctions de la CNIL, qui sont essentiellement financières. Celles-ci peuvent être analysées

950 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

selon deux aspects, d'abord la capacité de sanction financière directe de la CNIL (1), mais aussi les conséquences d'une remise en cause de la validité du consentement à l'aune de la décision de la Cour de Cassation du 25 juin 2013 (2).

1 – La capacité de sanction financière de la CNIL

612. Selon l'article 45 de la loi informatique et libertés modifiée : « *lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission Nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramenée à vingt-quatre heures* »[951]. Si le responsable de traitement ne se soumet pas à l'avis de l'autorité, un avertissement, une injonction de cesser le traitement ou une sanction pécuniaire peuvent être prononcés. Or, pour cette dernière, le montant est déterminant. En reprenant l'exemple de la décision de la CNIL contre la fusion des règles de confidentialité des services de Google[952], on s'aperçoit qu'il existe une grande disparité entre les capacités de sanctions de l'autorité indépendante et la profitabilité du modèle économique du géant Californien. En effet, pour une société de la taille de Google, le recours au montant maximum de sanction administrative infligé par la CNIL de 150 000€ parait faible. De fait, lorsque l'on ramène les bénéfices annuels de la société à une dimension temporelle, cela représente une perte d'à peine plus de 3 minutes de bénéfices[953].

613. Pour pallier ce déséquilibre, la loi du 7 octobre 2016 pour une République numérique a augmenté drastiquement le montant des sanctions pécuniaires[954]. Dorénavant, le montant maximum de la sanction est porté à trois millions d'euros. De plus le nouvel article 47 de la loi informatique et libertés dispose : « *le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des*

951 Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 45.
952 Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.
953 En se basant sur le bénéfice net pour l'exercice 2015 du géant Californien, 23 milliards de dollars.
954 Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.

libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable de traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission »[955]. Enfin, « *lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce* »[956]. A la lumière de ces évolutions, il apparait que tout revirement jurisprudentiel sur l'interprétation des critères de validité du consentement puisse avoir des répercutions économique bien plus importantes qu'auparavant, d'autant que cette loi intervient dans un contexte plus large de refonte des mécanismes de sanctions condamnant ce type d'infraction.

614. Après plusieurs années de négociations, le règlement général sur la protection des données a été publié au journal officiel de l'Union Européenne le 27 avril 2016. Celui-ci va plus loin que la loi Française pour la République numérique[957]. En fonction des circonstances de l'infraction[958], une amende pouvant aller jusque 10 000 000 € ou 2% du chiffre d'affaire mondial, selon le plus élevé, sera encourue si le responsable de traitement manque à ses obligations. En cas de violation des principes de bases d'un traitement, des droits dont bénéficient les personnes concernées, d'un transfert vers un pays tiers illicite, ou du non-

955 Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 47.
956 Ibid.
957 Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.
958 Sont ainsi visés : « *la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi; le fait que la violation a été commise délibérément ou par négligence; toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées; le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32; toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant; le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs; les catégories de données à caractère personnel concernées par la violation; la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation; lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures; l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation* », Ibid. article 83

respect d'une injonction, la sanction s'élève jusqu'à 20 000 000 € ou 4% du chiffre d'affaire annuel mondial.

615. Cette forte évolution du montant des sanctions parait, à première vue, une réponse cohérente aux limites du régime que nous avons exposées précédemment. Pourtant sur le fond, celui-ci repose uniquement sur la position jurisprudentielle du G29 et de la CNIL sur les critères de validité du consentement, dont nous avons démontré la faiblesse. Des lors, en augmentant le plafond des sanctions pécuniaires, le régime fragilise la pérennité des investissements dans l'innovation numérique, alors même que la sanction d'incessibilité des fichiers illicites pèse sur l'industrie.

2 - La sanction d'incessibilité des fichiers illicites

616. La CNIL dispose de la faculté d'adjoindre un responsable de traitement à cesser les traitements de données jugés illicites. Toutefois, cette sanction ne vaut que pour les traitements en cours et n'a pas d'effet rétroactif. De plus, la sanction n'est que rarement imposée lorsque l'on observe la jurisprudence de l'autorité indépendante. Entre 2014 et 2017[959], aucune des décisions publiques constatant un manquement à l'une des obligations de la loi informatique et libertés a entrainé la révocation du droit de traiter les données, quand bien même celles-ci avaient été obtenues de manière illicite, à l'instar de la décision contre Meetic du 15 décembre 2016[960]. En l'espèce, la CNIL constate que la procédure de recueil du consentement, concernant les données sensibles, ne respecte pas l'obligation de spécificité. En conséquence : « *la formation restreinte considère que le manquement à l'article 8 de la loi du 6 janvier 1978 modifiée a persisté au-delà du délai imparti par la mise en demeure de la présidente de la Commission et justifie que soit prononcée une sanction d'un montant de 20.000€ à l'encontre de la société* » [961].

959 Registre des sanctions prononcées par la Commission Nationale de l'Informatique et des Libertés, disponible sur https://www.cnil.fr/fr/les-sanctions-prononcees-par-la-cnil (consulté le 01/09/17).

960 Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.

961 Ibid.

617. Pourtant, la décision reste silencieuse sur le devenir des données acquises sur la période concernée. Selon toute logique, celles-ci devraient être détruites, puisque obtenues de manière illicite. Dans un pareil cas, l'ensemble du modèle économique serait fragilisé par la perte sèche de sa principale source de valeur, et pourrait même avoir des répercutions plus importantes si l'on prend en compte l'apport de la décision de la Cour de Cassation du 25 juin 2013[962]. En l'espèce, une société exploitante d'un fonds de commerce a fait l'acquisition d'un portefeuille de clientèle comprenant environ 6000 clients référencés. S'estimant lésé sur la qualité du fichier, celle-ci exerce une action visant à obtenir la nullité de la vente pour illicéité de l'objet. En effet, le traitement du fichier client devait faire l'objet d'une déclaration simplifié auprès de la CNIL, qui n'a pas été faite. Pour la Cour d'appel de Rennes: « *la loi n'a pas prévu que la sanction de l'absence de déclaration du traitement du fichier client soit la nullité du fichier* » [963] . elle rejette donc la demande de nullité. Cependant, selon la Cour de Cassation, dont l'argumentaire s'appuie sur une lecture rigoriste de l'article 1128 du Code Civil : « *le défaut de déclaration rendait le dossier illicite et, par la suite, la vente de ce dossier nulle pour objet illicite* » [964].

618. Or, la nullité pour objet illicite est une nullité absolue, avec un effet rétroactif et sans possibilité de régularisation. La cession n'a donc, juridiquement, jamais eu lieu, et la restitution des sommes perçues est automatique. De plus, il existe un véritable risque de contamination de l'ensemble de la transaction. Si le fichier était l'une des causes déterminantes d'une opération financière, la nullité peut être étendue à la totalité des transactions qui ont été réalisées autour de celui-ci. Enfin, les personnes concernées ont été victimes d'une communication frauduleuse de leurs données et, comme nous l'avons exprimé précédemment, celles-ci disposent de nombreux moyens pour obtenir réparation. D'abord au regard de la loi du 6 janvier 1978, puis selon l'article 9 du code Civil, et enfin, en vertu de l'article 226-16 du code pénal qui réprime « *le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formabilités préalables à leur mise en œuvre prévues par la loi [qu'il] puni de cinq ans d'emprisonnement et de 300 000 euro d'amende* ».

962 Cass. Com., 25 juin 2013, n°12-17037, Bull. Com. 2013, IV, n°108.
963 CA. Rennes, 17 janvier 2012, Répertoire Général n°10/07/599, arrêt n°15.
964 Cass. Com., 25 juin 2013, n°12-17037, Bull. Com. 2013, IV, n°108.

619. Des lors, les conséquences d'une requalification de la licéité d'une procédure de recueil du consentement dépassent la simple sanction pécuniaire de la CNIL, voir même l'infime possibilité que celle-ci demande à ce que les données obtenues antérieurement à la régularisation soient détruites. La sanction de nullité venant frapper toute transaction de fichier de données à caractère personnel illicite et atteint, rétroactivement, toute opération de valorisation qu'un responsable de traitement aura effectuée. Or, le modèle économique de l'innovation numérique repose sur cette faculté. Dans le cas d'une interprétation rigoriste de la portée de cette jurisprudence, on peut penser que pour chaque décision de la CNIL constatant une infraction au régime protecteur des données à caractère personnel, l'ensemble des opérations antérieures de valorisation soient nulles. Dans un pareil cas, chaque opérateur publicitaire ayant eu recours aux données d'un service internet tel que Google, Facebook ou Meetic (qui ont été condamnés), est en mesure de demander la restitution de l'ensemble des sommes versées.

Conclusion

620. En cherchant à trouver un équilibre entre droit au respect de la vie privée et pérennité d'un modèle économique favorable à l'innovation (basé sur la valorisation des données à caractère personnel), les législateurs Français et Européens ont choisi le consentement comme pivot juridique de cet écosystème. Des lors, le consentement devient l'outil principal de licéité et la solidité des critères qui le fondent est le principal facteur de sécurité juridique et économique.

621. Pourtant comme nous l'avons observé, cet engagement liminaire de l'utilisateur ne peut pas être considéré, sous sa forme actuelle, comme une représentation fidèle de sa volonté. Les critères qui définissent sa licéité peuvent être remis en question sur un plan doctrinal, mais peuvent également subir un revirement de jurisprudence dont les conséquences seraient désastreuses pour la pérennité de l'innovation technologique. En effet, lorsque l'on analyse les sanctions éventuelles qui pèsent sur le responsable de traitement en cas d'invalidation du consentement initial, c'est directement le modèle économique qui est atteint. D'abord par l'augmentation drastique des capacités de sanctions de la CNIL, puis par

les répercutions juridiques de la décision de la Cour de Cassation du 25 juin 2013[965]. Ainsi, dans l'éventualité d'un changement dans l'appréciation de la validité du consentement, la CNIL pourra déclarer illicite une procédure de recueil. Cette décision entrainera la nullité des opérations de valorisations antérieures, puis par corollaire, de toute utilisation ultérieure des données recueillies jusqu'à la mise en conformité. Pour la plupart des entreprises innovantes de l'informatique, une telle décision serait fatale. D'abord, parce que leur modèle économique est basé essentiellement sur la valorisation. Ensuite parce que leur valorisation dépend principalement de leurs bases de données utilisateurs. À titre d'exemple, on peut imaginer que l'opération de rachat de Whatsapp par Facebook en 2014 pour 22 milliards de dollars puisse souffrir grandement si la procédure intentée par la Commission Européenne relative aux infractions à la concurrence portant sur la fusion des bases de données ait un pendant dédié au respect du régime de protection des données à caractère personnel[966]. En supposant que le consentement des utilisateurs n'ait pas été respecté, la vente serait nulle.

622. Ainsi, la pérennité de l'innovation numérique repose sur un socle juridique friable, caractérisé par l'éventualité d'un revirement jurisprudentiel sur l'appréciation des critères de validité du consentement. Dans ce contexte, il parait opportun d'observer quelles peuvent être les mesures de refonte des mécanismes de protection de la vie privée dans l'innovation.

965 Cass. Com., 25 juin 2013, n°12-17037, Bull. Com. 2013, IV, n°108.

966 Commission Européenne, *Mergers: Commission's alleges Facebook provided misleading information about WhatsApp takeover*, IP/16/4473, Brussels, 20 December 2016.

Section 2

Pour une refonte des mécanismes de protection de la vie privée dans le cadre de l'innovation

623. Le régime, centré sur le consentement, fait face à ce que certains auteurs qualifient de *dilemme du consentement*[967]. D'un côté, le consentement est une reconnaissance de l'individualité, mais exploité par un responsable de traitement pour étendre ses possibilités de traitement, il devient un facteur de remise en cause des objectifs même du régime. De l'autre, une réglementation protectionniste limite de facto l'autonomie des personnes et leur capacité à choisir les données qu'ils souhaitent exposer. De plus, à la difficulté de trouver un équilibre entre ces deux options, Antoinette Baujard ajoute celle de qualifier ce qui constitue « *une bonne décision* ».

624. Ainsi, face à la possibilité d'une intervention législative limitant la capacité du consentement, « *les paternalistes font ce qu'ils pensent être bon, et ne demandent pas l'avis des personnes concernées. Le Paternalisme est une notion liée à la tradition Kantienne parce qu'elle s'oppose au principe d'égalité dans le traitement de la volonté des personnes, dans le sens où celle-ci doit être vue comme une fin en soi (Dworkin 2014). J'affirme que ces personnes sont à peine considérées comme des fins en soi, étant donné que ceux qui définissent les politiques publiques ne leur demandent pas leur consentement et ne les impliquent pas dans les processus de décision* »[968]. Dès lors, toute décision qui serait prise par

967 v. Therrien Daniel, Privacy Commissioner of Canada, *Speak recorded at the Privacy & Laws & Business 29th Annual Internal Conference*, Cambridge, 2-6 July 2016 ; Baujard Antoinette, *Beyond the Consent Dilemma in Libertarian Paternalism, a Normative Void*, *Homo Oeconomicus*, Accedo Verlag, 2015, pp. 301-305. ; Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, pp. 141-165 ; Acquisti Alessandro, Grossklags Jens, *What Can Behavioral Economics Teach Us About Privacy?*, Digital Privacy: Theory, Technologies and Practices, Taylor and Francis Group, 2007, pp. 160-179.

968 Traduction par l'auteur de : « *Paternalists do as if they knew what is good, and do not wonder about the views of people concerned. Paternalism is an issue according to the Kantian tradition because it conflicts with a principle of equal respect of persons, in the sense that persons should be treated as ends in themselves (Dworkin 2014). I claim that persons are hardly being considered as ends by those who design public policy when the latter do not ask about their consent, and do not involve them in the decision process* ». Baujard Antoinette, *Beyond the Consent Dilemma in Libertarian Paternalism, a Normative Void*, *Homo Oeconomicus*, Accedo Verlag, 2015, pp. 301-305.

une entité supérieure à l'individu lui-même ne pourrait être légitime à définir ce qui lui est bon. Pourtant à l'inverse, si l'on place l'individu dans une situation d'infériorité, la décision qu'il pourrait prendre peut être contraire à ses intérêts. Dans ces conditions, comment définir la légitimité et les bornes d'une intervention législative protectrice qui chercherait à limiter les choix des personnes ?

625. En réalité, deux visions s'opposent. La première consacre la liberté individuelle comme valeur cardinale du droit, idée selon laquelle le consentement reste un mode d'expression incontestable de la volonté individuelle, seule capable d'exprimer un choix favorable à l'individu pour lui-même. La seconde est partisane d'une approche sociale du droit, considérant que la vision précédente est dépassée par les changements techniques et sociaux qui suggèrent un affaiblissement de la capacité des personnes à effectuer des choix qui leurs sont favorables, notamment lorsqu'ils sont confronté à des situations dans lesquelles le rapport de force est asymétrique. Par conséquent, toute proposition de refonte du régime est nécessairement polarisée.

626. Pour éviter cet écueil, il nous faut adopter une position médiane. Ainsi selon Jean-Pascal Chazal : « *la majorité des professeurs de droit, quelles que soient leurs opinions politiques (droit ou gauche) ou leurs convictions religieuses (catholique ou non), adoptent une position conciliatrice, médiane. Ils souhaitent ardemment préserver l'ordre social, mais ils consentent, ou bien avec conviction ou bien par fatalisme ou encore par intelligence tactique, à des transformations du droit. C'est en ce sens que le droit se socialise : il s'ouvre sur la question sociale ; laquelle implique que les solutions juridiques ne soient plus seulement déduites des règles abstraites et ancestrales compilées dans le Code Civil, mais aussi et peut être surtout, construites par un raisonnement inductif qui prend ses racines dans les faits, dans la société* »[969]. Il ne s'agit donc pas de renier en bloc le consentement, ni d'imposer une forme de paternalisme juridique, mais bien d'adresser point par point, les faiblesses du régime. En l'espèce, analyser les solutions qui permettent de redonner aux personnes concernées une véritable protection, sans oublier les aspects économiques et techniques qui dépendent de cette qualification. Dans ce contexte, une meilleure protection est

969 Chazal Jean-Pascal, *La protection de la partie faible chez Josserand, ou la tentative de maintenir le compromis républicain*, Un ordre juridique Nouveau ? Dialogue avec Louis Josserand, dir. Dross William, Favario Thierry, Mare et Martin, 2014, p. 228.

synonyme d'une amélioration de la sécurité juridique et la solution la plus efficace sera celle qui saura concilier ces deux objectifs. Pour cela, il est nécessaire d'observer les propositions de modifications des critères de validité du consentement (1) avant d'envisager une refonte des mécanismes de protections du régime (2).

1 – Les propositions de modifications des critères de validité du consentement

627. Publié le 27 avril 2016 et applicable à partir du 25 mai 2018, Le nouveau règlement général sur la protection des données a pour objectif assumé de redonner le contrôle de leurs données aux citoyens[970]. Il s'accompagne de mesures tendant à confirmer les positions jurisprudentielles concernant le consentement et à qualifier avec plus de précision les critères qu'elles avaient définis. En ce qui concerne la spécificité du traitement, le considérant 32 reprend la logique initiale. Selon celui-ci : « *Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé* » [971]. Sur l'obligation d'information, le considérant 42 indique que « *pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel* »[972].

628. Si ces nouvelles définitions ont une portée relative, une réelle nouveauté apparait dans le renforcement des dispositions ayant trait à la liberté de consentir. Avec l'article 7-4, le règlement impose une nouvelle manière d'évaluer la liberté de consentir applicable aux

970 Commission Nationale de l'Informatique et des libertés, *Règlement Européen : ce qui change pour les professionnel, Communication du 15 juin 2016*, disponible sur https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels (consulté le 01/09/17).

971 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

972 Ibid, considerant 32.

conditions générales de service, en prenant en compte le sentiment de dépendance qu'un utilisateur peut expérimenter au moment d'autoriser un service à collecter ses données. Ainsi : « *Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat* » [973]. De plus, le règlement indique dans son considérant 42 que « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice* » [974]. De même dans le considérant 43, il est indiqué que « *pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière* ». Enfin, « *le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution* » [975].

629. Afin d'affirmer ses objectifs de protection des utilisateurs, le règlement apporte également des modifications aux conditions de forme. Ainsi le considérant 32 impose que « *le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale* » [976]. Il confirme ainsi la

973 Ibid, article 7-4.
974 Ibid, considerant 42.
975 Ibid, considerant 43.
976 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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1, considérant 32.

jurisprudence précédente du G29, tout en proposant de nouvelles modalité pour la mise en place de cette procédure : « *Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors, y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité* » [977]. Si l'ensemble de la définition est proche de celle actuellement en vigueur, la dernière phrase semble amorcer une refonte du système applicable aux Cookies, en supprimant la possibilité de considérer la continuation de la navigation comme un consentement à l'exploitation des données.

630. Enfin, selon l'article 7 : « *dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant* » [978]. Cela correspond à la nécessité pour le responsable de traitement d'enregistrer de manière systématique le consentement de la personne, et d'associer ce consentement aux données collectées. Avec cette exigence, le règlement facilite le travail en aval des autorités indépendantes lors du contrôle de la licéité des traitements.

631. Le règlement Européen semble apporter des précisions importantes quant à la qualification du consentement en prenant en compte l'asymétrie existante entre un utilisateur et le responsable de traitement. Cette nouvelle définition étendue de la liberté de consentir, implique une stricte séparation des finalités du traitement et de la fourniture de service. Toutefois, il ne termine pas son analyse en définissant avec plus de précision les modalités d'analyse de la distinction des finalités, ni des facteurs qualifiant la liberté de consentir. A titre d'exemple, un service social tel que Facebook nécessite l'accord de la personne concernée pour traiter ses données, pour lui permettre de créer un profil, de dialoguer et de partager des informations. Mais cette finalité autorise, par la même occasion, le service à valoriser les données. Dans ce cas, l'exécution du service est difficilement séparable de la nécessité de partager des informations. Appliqué à cet exemple, le critère de liberté, ainsi

977 Ibid.
978 Ibid, article 7.

défini par le règlement, ne prend pas en compte l'impact social que revêt l'abandon du réseau pour un utilisateur, et la nouvelle définition concernant la finalité ne permet pas de faire la distinction entre la finalité de traitement nécessaire à l'utilisation du service et la finalité commerciale associée.

632. De la même manière, la possibilité d'utiliser le comportement comme critère de qualification de la volonté de consentir reste ouverte « *dans un contexte* » déterminé, malgré l'interdiction de recourir au silence ou à l'inactivité. Dès lors, la définition semble, une nouvelle fois, sous le jouc d'un revirement jurisprudentiel en fonction de l'appréciation de ce comportement, d'autant que le règlement ne fait qu'abroger la directive 95/46/CE[979] sans remettre en cause la directive 2009/136/CE dont l'article 5(3) vise explicitement cette technologie[980]. Faut-il conclure que le fait de continuer la navigation sur un site internet est toujours susceptible de qualifier le consentement à l'exploitation des données ?

633. Il est donc possible, malgré ces nouveaux critères, de reprendre notre analyse développée précédemment, et de critiquer avec les mêmes arguments le manque de discernement de la nouvelle politique Européenne. En définitive, le renforcement des règles de licéités du consentement ne fait que rééditer la controverse initiale portant sur l'information, la liberté et la spécificité du consentement. La problématique de l'asymétrie informationnelle n'est d'ailleurs toujours pas résolue, puisque notre observation initiale est toujours valable. La liberté de consentir, bien que renforcée, manque d'une détermination plus efficace des finalités de traitement. Au final, le règlement général sur la protection des données ne fait que créer l'illusion d'une spécificité de consentement réaffirmée, alors qu'il ne s'agit que d'une modification cosmétique.

979 Directive n°31995L0046 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

980 Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009, *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal Officiel de l'Union Européenne n°L337/11, 18 décembre 2009.

634. La jurisprudence peut cependant pallier ces oublis. En faisant la distinction des finalités d'exploitation d'un service par l'utilisateur, et la commercialisation de ses données, la CNIL est capable, sur la base de ce nouveau texte, de redonner aux citoyens Français le contrôle de leurs données. Dans un telle perspective, les conséquences sur l'économie numérique seraient dévastatrices, puisque l'on peut supposer qu'un certains nombres d'internautes prendraient la décision d'accéder à un service sans autoriser pour autant la valorisation des données. La viabilité d'un site internet tel que Facebook, dépendant presque entièrement des revenus publicitaires, serait alors gravement entamée, au-delà même des conséquences d'une remise en cause de la validité de la procédure de recueil initiale, que nous avions exposé précédemment. Dans une pareil éventualité, il faut imager la possibilité que les services offre deux versions d'un même service. L'une sans que les données de l'utilisateur soient traitées, et une seconde dépendant du consentement de l'utilisateur, avec valorisation.

635. Par conséquent, la proposition Européenne de refonte des critères du consentement, qui sera applicable en 2018, est porteuse d'une grande insécurité juridique alors même que la protection des personnes concernées reste faible. Dans un tel contexte, une simple réinterprétation de la condition de spécificité du consentement remettrait en cause l'architecture même des principaux services internet.

2 – Pour une refonte des mécanismes de protection de la vie privée dans l'innovation technologique

636. À travers sa réforme du consentement, le règlement général sur la protection des données ne palie pas les faiblesses structurelles du régime. Au contraire, en tentant de renforcer maladroitement cette notion sans redéfinir les autres facteurs de protection, le nouveau régime augmente le risque juridique pesant sur l'innovation technologique et la protection de la vie privée des citoyens. Dans ce contexte, toute tentative de refonte des mécanismes de protection s'attachant à répondre à cette problématique en conservant le système actuel ne ferait que reproduire ces défauts.

637. Il faut donc se rendre à l'évidence, quels que soient ses critères de définition, le consentement ne peut pas, à lui seul, constituer une protection suffisante de la vie privée à l'ère numérique. Selon Eleni Kosta : *« spécialement dans le domaine des communications électroniques et dans le monde numérique en général, l'utilisation du consentement pour le traitement de données à caractère personnel ou pour effectuer une action qui serait autrement constitutive d'une atteinte à la vie privée de la personne concernée n'est pas toujours un moyens de protection suffisant. En réalité, on peut avancer l'idée que celui-ci tend d'avantage à devenir une procédure bureaucratique ou une justification paresseuse [pour les responsables de traitement]* »[981]. Il convient donc d'imaginer d'autres mesures de protection.

638. L'une des solutions serait de renforcer les autres conditions de licéité du traitement. Selon Gabriela Zanfir: « *si nous acceptons le fait que le rôle du consentement dans la protection des données est réduit, alors le droit à la protection des données a besoin, autant en pratique qu'en théorie, de reposer sur d'autres prérogatives spécifiques afin que son objectif soit atteint* » [982]. Toutefois, la faiblesse de cette approche réside dans le fait que ces autres prérogatives évoquées, telles que les droits de la personne concernée ou l'exigence de proportionnalité du traitement existent déjà sans produire d'effets suffisamment restrictifs pour empêcher les abus que nous avons constatés.

639. Dès lors, la seule option possible reste celle d'une remise à plat de la structure juridique de protection de la vie privée dans l'innovation numérique. Nous avions démontré en première partie que la conception même de la vie privée dans l'innovation numérique était porteuse d'une réduction conceptuelle, en troquant le droit au respect de la vie privée pour celui du régime applicable aux données à caractère personnel. L'une des solutions possibles, serait donc de ramener ce régime spécial sous le joug de celui de la vie privée, en considérant celui-ci comme un simple périmètre décisionnel informationnel. Cela permettrait d'introduire

981 Traduction de l'auteur de : *«Especially in the electronic communications sector and the online world in general the reliance on consent for the processing of personal data or the carrying out of an action that would otherwise constitute a violation to the privacy of the data subject does not always safeguard the protection of his privacy. In fact, I can be argued that there is currently a tendency to make use of consent as both parts of a bureaucratic process and as a lazy justification ».* Kosta Eleni, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, 21 mars 2013, p. 395.

982 Traduction de l'auteur de : *«If we accept that the role of consent in data protection is reduced, then the right to the protection of personal data needs, both in theory and in practice, to rely on other specific and well defined prerogatives of the data subject so that its purpose is achieved ».* Zanfir Gabriela, *Forgetting about consent: why the focus should be on suitable safeguards in data protection law*, University of Craiova, May 2013, p. 20.

dans le monde numérique la dimension première de notre définition de la vie privée, la faculté d'autonomisation de la volonté individuelle, sans pour autant la réduire à la faculté d'utiliser ou non des données à caractère personnel. À défaut d'effacer l'ensemble des failles structurelles du régime, le recours à cette définition autorise les juges du fonds et les autorités indépendantes à confronter à une nouvelle matrice les atteintes à la vie privée numérique, englobant la faculté de développement personnel. Dans cette perspective, les contrôles a posteriori seraient en mesure d'apprécier l'impact des différents traitements de données, non seulement dans la sphère d'utilisation régalienne avec l'utilisation des technologies de surveillance, mais également dans la sphère publique avec l'évaluation de la licéité des bulles informationnelles.

640. Toutefois, en suivant cette conception, il devient du devoir du législateur de déterminer avec exactitude la seconde partie de notre définition de la vie privée, le périmètre décisionnel informationnel de la personne. Ainsi, au lieu d'offrir un périmètre illimité dans la disponibilité de ses propres données, une concertation Européenne en la matière pourrait définir des bornes à l'exploitation des données, ou du moins, à la valorisation de certaines d'entre elles. Face aux conditions d'utilisation de Google qui s'arrogent le droit d'établir une collecte extrêmement vaste, on pourrait imposer par exemple une double limitation, d'abord dans celle de l'utilisation des données dites « *sensibles* », puis une distinction entre l'autorisation d'utiliser les données pour les besoins du service et la valorisation.

641. Cette solution aurait toutefois pour effet de diminuer drastiquement la rentabilité des GAFA, dont l'économie première reste celle de la donnée. Cependant, si l'on considère que le droit au respect de la vie privée doit survivre dans l'univers numérique, la vision pragmatique de l'utilisation du droit dans son environnement concret suggère d'adopter des mesures restrictives en matière d'utilisation des données.

Conclusion

642. Le régime applicable aux données à caractère personnel semble représenter ce que Lacordaire cherchait à exprimer par sa célèbre maxime : « *entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime, et la loi qui affranchit* »[983]. Dans un environnement numérique où l'utilisateur est constamment confronté aux conditions générales d'utilisation des données, le consentement est victime d'une véritable réduction de valeur. Par conséquent, une remise en cause des mécanismes de protection juridique est nécessaire, en adaptant son périmètre à celui des abus dont il est l'objet.

643. Pour cette raison, le recours à notre proposition de définition de la vie privée permet de répondre à cette problématique. D'une part en réaffirmant la place du droit au respect de la vie privée dans le monde numérique, d'autre part en redéfinissant le périmètre décisionnel de la personne concernée ou du responsable de traitement dans la libre collecte et la libre définition des objectifs du traitement.

983 Lacordaire Henri, *Conférences de Notre-Dame de Paris*, Sagnier et Bray, 1848, p. 246.

Conclusion Partie II

644. L'adaptation des acteurs de l'innovation au régime des données à caractère personnel a eu une influence considérable sur la manière dont celui-ci protège les citoyens. En érigeant le consentement comme élément principal de licéité, les législateurs Français et Européens ont généré un phénomène de généralisation des conditions générales de service, incluant celui d'une mise en place systématique des règles de confidentialité définissant l'usage des données. Or, de par la maîtrise rédactionnelle qu'ont les principaux fournisseurs de services informatiques sur celles-ci, internet s'est peu à peu transformé en un espace dont l'utilisation n'est plus libre, mais conditionnée à l'acceptation généralisée de l'exploitation des données.

645. À l'intérieur de cet espace numérique, le droit au respect de la vie privée fait l'objet d'une véritable réduction à travers le critère de consentement préalable au traitement, devenu une obligation cosmétique plutôt qu'un représentant fidèle de la volonté de l'utilisateur

Conclusion générale

646. Comme nous l'avons observé en introduction, la principale difficulté concernant l'étude de la prise en compte de la vie privée dans l'innovation technologique naît de l'absence d'une définition générale du droit au respect de la vie privée. Ainsi, si l'on peut trouver celle-ci dans le code civil ou dans la jurisprudence[984], les rédacteurs évitent systématiquement de circonscrire la notion. Dans ce contexte, comment juger de l'efficacité d'une protection sans savoir réellement ce qui doit être protégé ?

647. C'est en cela que notre approche est novatrice. Plutôt que de décrire une nouvelle fois le régime applicable aux données à caractère personnel, nous avons créé dans la première partie un point fixe à partir duquel nous pouvons juger de sa pertinence : une définition générale de la vie privée, construite à partir de l'observation de la jurisprudence, de la doctrine et de l'évolution de la société. Celle-ci s'articule autour de deux concepts : une protection de la faculté d'autonomisation de l'individu et le périmètre décisionnel qui lui est accordé. Décrite de manière succincte, la protection de la faculté d'autonomisation de l'individu est l'ensemble des éléments permettant à un individu de décider pour lui-même en dehors de toute sphère d'influence. Cela comprend la notion de développement personnel ainsi que les interactions et les connaissances nécessaires. Le périmètre décisionnel, quant à lui, constitue la limite que la société fixe pour l'exercice des choix de l'individu. Dans cette conception juridique, la protection de la vie privée pourrait être ainsi résumée : la garantie qu'un individu puisse se construire selon toute la latitude des possibilités humaines, mais que la société puisse fixer les limites de son territoire décisionnel.

648. Partant de cette définition, nous avons ensuite cherché à évaluer l'efficacité de la protection offerte par le droit dans l'innovation numérique. Nous avons constaté qu'au lieu d'intégrer le numérique à la protection générale, les législations françaises et européennes ont réduit sa portée en créant un régime sui generis : celui des données à caractère personnel.

984 v. Introduction et Partie I, Titre I, Chapitre I.

649. Cela sert de matière à la conclusion de la première partie de notre étude : la prise en compte de la vie privée dans l'innovation numérique ne saurait se résumer à la protection des données à caractère personnel. En focalisant son attention sur ce régime, le législateur semble s'enfoncer dans un paradigme qui ne permet pas de qualifier l'impact du numérique sur la vie privée dans toute sa mesure. Il s'agit d'un régime distinct qui, bien qu'empruntant les mêmes termes, ne couvre qu'une infime partie de son essence. Cela fragilise la protection offerte aux citoyens en laissant la possibilité à de nouvelles atteintes numériques de se perpétrer sans que le droit puisse les appréhender et sans que la technologie puisse valablement y répondre.

650. Cette première partie portant sur l'efficacité de l'adaptation du droit à un phénomène technologique devait nécessairement s'accompagner d'une étude sur l'adaptation des acteurs de l'innovation au régime de protection. En effet, si l'on peut déplorer ses défauts théoriques, le régime applicable aux données à caractère personnel a favorisé l'émergence de nouveaux outils numériques au service de l'économie et des citoyens. Il offre également la possibilité aux services numériques de s'investir dans la protection des données en intégrant de nouvelles exigences au cœur des processus d'innovation.

651. Pour juger de cette faculté du régime, nous avons analysé l'exigence de recueil préalable du consentement qui, au lieu d'être un simple critère de licéité des traitements parmi d'autres, se trouve être la raison principale pour laquelle les différents services numériques ont déployé des conditions d'utilisations du service. Qu'il s'agisse d'un simple site internet disposant d'outils de suivi de l'internaute (Cookies), d'interfaces de programmation applicative (API) ou d'un moteur de recherche, le citoyen est aujourd'hui contraint d'accepter la collecte et le traitement de ses données en échange d'un accès numérique.

652. Or, cela conduit à s'interroger sur la pertinence du choix du législateur dans l'établissement de ce modèle de protection. Il laisse l'individu seul responsable de la protection de ses données face à des conditions générales d'utilisation particulièrement libérales en matière d'exploitation de celles-ci. De plus, il apparait que les conditions de licéité du consentement ne sont pas suffisantes pour s'assurer de la représentation fidèle d'une volonté libre et éclairée. Les exigences de liberté, de spécificité et de consentement éclairé ne sauraient être respectées face aux difficultés techniques et cognitives qu'elles représentent, et

les apports du nouveau règlement général sur la protection des données ne pallient pas ces faiblesses. Cela entraine un affaiblissement de la valeur du consentement dans l'innovation technologique qui le transforme en facteur d'insécurité juridique, porteur d'un risque pour le respect de la vie privée des citoyens, mais aussi en menace pesant sur la pérennité de l'économie numérique.

653. Face à cette problématique juridique structurelle, l'apport de la Privacy By Design semble limité voire dangereux. En introduisant une faculté pour l'industrie de définir des protections techniques à l'exploitation abusive de données à caractère personnel, il offre la possibilité d'une coordination opportuniste qui favoriserait les exploitants au détriment des personnes concernées. Cela représente un transfert de la capacité normative, du législateur vers l'industrie, qui aura pour effet de laisser certains pans de l'innovation à la merci de comportements frauduleux, faute d'une protection définie. Dans cette seconde partie, nous sommes forcé de conclure que la fragilité du régime, caractérisée par la perte de valeur du consentement et par l'inaptitude de la Privacy By Design à y répondre, va jusqu'à remettre en question la solidité du modèle économique dominant dans l'innovation numérique.

654. Ainsi, la conclusion de notre étude ne peut aller que dans un sens : la seule solution susceptible de compenser les faiblesses structurelles du régime est un changement de paradigme portant sur la définition de la vie privée. En adoptant la conception que nous proposons, le régime des données à caractère personnel redevient spécifique et le droit au respect de la vie privée peut s'appliquer de manière plus large dans le numérique. Ce faisant, nous offrons une meilleure protection au citoyen, autant dans le monde numérique que dans le monde « *réel* ». Ce n'est qu'à ce prix que la confiance des citoyens dans les mécanismes de protection se trouvera justifiée et que l'innovation numérique disposera d'un socle juridique suffisamment solide pour être durable.

655. Pour autant, notre proposition ne peut s'envisager qu'avec un travail de co-construction conceptuelle, relevant de plusieurs disciplines tant juridique que sociologique, voire philosophique. Tout d'abord, elle implique, pour la première partie de la définition portant sur la protection de la faculté d'autonomisation, de préciser les éléments cognitifs qui permettent à un individu d'acquérir cette faculté. La liberté de circuler, de communiquer, l'éducation et l'accès à une information neutre en font partie intégrante. Sur ces points, les

réflexions actuellement menées aux Etats Unis, en lien avec l'affaire des publicités russes sur les réseaux sociaux, accusées d'avoir influencé l'issue de l'élection américaine, peuvent être instructives[985]. Mais comment qualifier le socle minimum de la faculté d'autonomisation ? Les solutions que semblent présenter les « *nudges* »[986] dans ce domaine ne peuvent que laisser dubitatif, puisque l'influence des décisions humaines est peu compatible avec l'idée d'une volonté libre. De plus, une autre difficulté provient de la seconde partie de la définition : le périmètre décisionnel. Entre le besoin économique vital de la valorisation des données pour l'innovation numérique et une protection efficace de la vie privée des personnes concernées, comment définir un périmètre décisionnel équilibré ?

656. Notre réflexion sur la solution que nous mettons en avant dans cet ouvrage n'a pas vocation, en l'état, à répondre à l'ensemble de ces problématiques. De nombreux points méritent un débat plus large, tant la question d'une définition générale de la vie privée est cruciale pour la société et pour l'ordre juridique. Mais si celle-ci engendre des difficultés d'ordre juridiques, sociologiques et philosophiques importantes, elle propose un nouvel outil permettant de renforcer la protection de la vie privée. La pertinence de son déploiement peut donc se résumer à une interrogation : si nous ne sommes pas satisfaits de la protection de la vie privée, n'est-il pas temps de changer de paradigme de protection ?

985 Le Monde.fr, *Publicités électorales russes : Facebook détaille ce qu'il a remis au Congrès américain*, 3 octobre 2017, disponible sur http://abonnes.lemonde.fr/pixels/article/2017/10/03/publicites-electorales-russes-facebook-detaille-ce-qu-il-a-remis-au-congres-americain_5195456_4408996.html (consulté le 01/11/19)

986 Cappelli Patrick, *Les Nudges, Force de persuasion*, 19 janvier 2014, disponible sur http://www.liberation.fr/futurs/2014/01/19/les-nudges-force-de-persuasion_973983 (consulté le 01/09/17).

Bibliographie

I - Ouvrages

About Ilsen, Denis Vincent, *Histoire de l'Identification des Personnes*, La Découverte, 27 mai 2010, 128 p.

Arendt Hannah *Responsabilité et Jugement*, Payot, 5 mars 2009, 362 p.

Arendt Hannah, *Condition de l'Homme Moderne*, Pocket, 28 Août 2002, 416 p.

Aristote, *Ethique à Nicomaque*, Vrin, 1 janvier 1994, 540 p.

Babinet Gilles, *L'Ere Numérique, Un Nouvel âge de l'Humanité : Cinq Mutations Qui Vont Bouleverser Notre Vie*, Le Passeur éditeur, janvier 2014, 236 p.

Bentham Jeremy, *An introduction to The Principles of Morals and Legislation*, Courier Corporation, 7 mars 2012, 416 p.

Bitan Hubert, *Droit et expertise du numérique*, Lamy Axe Droit, 11 juin 2015, 650 p.

Black Edwin, *IBM et l'Holocauste, l'Alliance Stratégique entre l'Allemagne Nazie et la Plus Puissante Multinationale Américaine*, Robert Laffont, 13 février 2001, 610 p.

Bonnaventure de Roquefort Jean Baptiste, *Dictionnaire Etymologique de la Langue Françoise*, Volume 1, Décourchant, 1829, 462 p.

Borking John, Van Eck B.M.A, Spiepel P., *Intelligent Software Agents and Privacy*, Registratiekamer, The Hague, janvier 1999, 73 p.

Bourdieu Pierre, *Le Sens Pratique*, Les Editions de Minuit, 1 février 1980, 500 p.

Bravo Alain, *La Société et l'Economie à l'Aune de la Révolution Numérique : Enjeux et Perspectives des Prochaines Décennies*, La Documentation Française, 29 octobre 2009, 102 p.

Carbonnier Jean, *Droit Civil*, vol. 1, PUF, 8 octobre 2004, 2573 p.

Castells Manuel, *La Société en Réseaux*, Fayard, 21 février 2001, 674 p.

Catala Pierre, *Le Droit à l'Epreuve du Numérique : Jus Ex Machina*, PUF, 25 septembre 2015, 345 p.

Cavoukian Ann, *Operationalizing Privacy by Design: A guide to Implementing strong privacy practices*, Information and Privacy Commission, December 2012, 74 p.

Charton Eric, *Hacker's Guide*, Pearson Education, 22 Août 2013, 324 p.

Clément F.B., *Philosophie Sociale de la Bible*, Paul Mellier Editeur, 1848, 444 p.

Cornu Gérard, *Vocabulaire Juridique,* PUF, 13 janvier 2016, 1152 p.

Cozette Philippe, *Programmer pour Internet : Notions fondamentales et Mise en Pratique*, Editions ENI, 6 février 2007, 633 p.

Cukier Kenneth, Mayer-Schoenberger Viktor, *Big Data : La Révolution des Données est en Marche*, Robert Laffont, 20 février 2014, 300 p.

Curien Nicolas, Muet Pierre-Alain, *La Société de l'Information*, La documentation Française, 2004, 312 p.

Deleuze Gilles, *Empirisme et Subjectivité*, PUF, 13 octobre 2010, 160 p.

Dick Philip K., *Minority Report*, Folio, 4 juin 2009, 272 p.

Durkheim Emile, *Les Règles de la Méthode Sociologique*, Flammarion, 10 Mars 2010, 333 p.

Ellul Jacques, *Le Système Technicien*, Calmann-Lévy, 1 avril 1994, 361 p.

Engebretson Patrick, *Les Bases du Hacking*, Pearson, 23 Août 2013, 240 p.

Foucault Michel, *Sécurité, Territoire, Population*, Le Seuil, 1 octobre 2004, 448 p.

Foucault Michel, *Surveiller et Punir,* Gallimard, 20 février 1975, 352 p.

Frayssinet Jean*, Informatique, Fichiers et Libertés : Les Règles, Les Sanctions, La Doctrine de la CNIL*, Litec, 1 janvier 1992, 229 p.

Gates Bill, *La Route du Future*, Pocket, 2 janvier 1997, 332 p.

Gaudrat Philippe, Sardain Frederic, *Traité de droit civil du numérique : Tome 1*, Larcier, 13 octobre 2015, 906 p.

Gounot Emmanuel, *Le principe de l'Autonomie de la Volonté en Droit Privé,* A. Rousseau Editeur, 1912, 470 p.

Greenwald Glenn, *Nulle Part où se Cacher*, JC Lattès, 14 mai 2014, 280 p.

Grynbaum Luc, Goffic Caroline (le), Morlet Lydia-Haidara, *Droit des Activités Numériques*, Dalloz, 25 juin 2014, 1054 p.

Heidegger Martin, *Etre et Temps*, Gallimard, 12 novembre 1986, 600 p.

Hume David, *Traité de la Nature Humaine : Livre 1 et appendice, l'Entendement*, Flammarion, 4 janvier 1999, 433 p.

Kahneman Daniel, Slovic Paul and Tversky Amos, *Judgment under Uncertainty, Heuristic and Biases*, Cambridge University Press, 20 mai 1982, 544 p.

Kahneman Daniel, *Thinking Fast and Slow*, Penguin, 10 mai 2012, 512 p.

Kant Emmanuel, *Critique de la Raison Pure*, Flammarion, 18 août 2006, 749 p.

Kosta Eleni, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, 21 mars 2013, 434 p.

Lacordaire Henri*, Conférences de Notre-Dame de Paris*, Sagnier et Bray, 1848, 658 p.

Lavenue Jean-Jacques, Villalba Bruno, *Vidéo-surveillance et Détection Automatique des Comportements Anormaux*, Septentrion, juillet 2011, 294 p.

Lee John A. N., *International Biographical Dictionary of Computer Pioneers*, Taylor & Francis, 1 novembre 1995, 830 p.

Lemberger Pirmin, Batty Marc, Morel Médéric, Raffaelli Jean-Luc, *Big Data et Machine Learning : Manuel du Data Scientist*, Dunod, 18 février 2015, 240 p.

Lepage Agathe, *Libertés et Droits Fondamentaux à l'Epreuve de l'Internet*, Lexis-Nexis, 3 février 2003, 328 p.

Loukouman Amidou, *Marketing des Réseaux Sociaux*, MA Editions, 22 février 2012, 264 p.

Lucas Michael, *PGP et GPG : Assurer la Confidentialité de ses E-mails et Fichiers*, Eyrolles, 31 août 2006, 248 p.

MacFarlane Nigel, *Firefox à 200%*, O'Reilly, 7 Juillet 2005, 194 p.

Martin Lucien, *Le Secret de la Vie Privée*, Sirey, 1959, 256 p.

Martin Xavier, *Nature Humaine et Révolution Française*, Martin Morin, 24 septembre 2015, 308 p.

Mayer-Schonberger Viktor, Cukier Kenneth, *Big Data : A Revolution that Will Transform How We Live, Work and Think*, Eamon Dolan and Houghting Mifflin Harcourt, 5 mars 2013, 256 p.

Mayeur Jean-Marie, *La Vie Politique sous la Troisième République (1870-1940),* Seuil, 1 avril 1984, 445 p.

Mill John Stuart, *De la Liberté*, Jean-Marie Tremblay, 19 mai 2002, 88 p.

Montaigne Michel (de), *Les Essais*, PUF, 9 juillet 2004, 1504 p.

Mutyaba Robert, *Improving the RSA Cryptographic Algorithm*, Lambert Academic Publishing, 2010, 84 p.

Neveu Erik, *Une Société de Communication ?,* Montchrestien, 15 juin 2011, 160 p.

Orwell George, *1984*, Gallimard, 16 décembre 1972, 438 p.

Orwell George, *La Ferme des Animaux*, Belin – Gallimard, 22 août 2013, 192 p.

Pariser Eli, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin, 1 mars 2012, 304 p.

Ranouil Véronique*, L'Autonomie de la Volonté : Naissance et Evolution d'un Concept*, PUF, 1980, 165 p.

Rogosch Patricia, Hohl Erik, *Data Protection and Facebook: An Empirical Analysis of the Role of Consent in Social Network,s* LIT Verlag, 10 octobre 2012, 72 p.

Roques-bonnet Marie-Charlotte, *Le Droit Peut-il Ignorer La Révolution Numérique ?*, Michalon, 4 novembre 2010, 606 p.

Roussillon Henry, *Liberté Personnelle: une Autre Conception de la Liberté ?*, Presses de l'Université des Sciences Sociales de Toulouse, 1 juin 2006, 159 p.

Schopenhauer Arthur, *Essai sur le Libre Arbitre*, Rivages, 2 mars 1992, 176 p.

Terestchenko Michel, *Un si Fragile Vernis d'Humanité*, La Découverte, 4 octobre 2007, 308 p.

Thaler Richard H, *Nudge: Improving Decision About Health, Wealth and Happiness*, Penguin, 24 février 2009, 320 p.

Turk Alex, *La Vie Privée en Péril : Des Citoyens sous Contrôle*, Odile Jacob, 17 mars 2011, 272 p.

Untersinger Martin, *Anonymat sur internet : Protéger sa vie privée*, Editions Eyrolles, 29 octobre 2014. 264 p.

Vindé Francois*, L'Affaire des Fiches, 1900-1904 : Chronique d'un Scandale*, Editions Universitaires, 22 décembre 1989, 236 p.

Walliser Bernard, *Economie et Cognition*, Editions Odile Jacob, 25 Août 2008, 263 p.

Walls Colin, *Embedded Software: The Works*, Newnes, 18 octobre 2005, 416 p.

II - Articles

1 - Articles Scientifiques

Acquisti Alessandro, Grossklags Jens, *What Can Behavioral Economics Teach Us About Privacy?*, Digital Privacy: Theory, Technologies and Practices, Taylor and Francis Group, 2007, pp. 160-179.

Ailincai Michaela, *Espoirs et Inquiétudes Autour de la Révision du Cadre Juridique Général de l'Union Européenne sur la Protection des Données à Caractère Personnel*, Revue de l'Union Européenne n°576, mars 2014, pp. 170-177.

Badinter Robert, *Le Droit au Respect de la Vie privée*, JCP G 1968, I, 2136, n°22.

Balleys Claire, Coll Sami**,** *La Mise en Scène de la Vie Privée en Ligne par les Adolescents*, *RESET*, 2015, disponible sur http://reset.revues.org/547 (consulté le 01/09/17).

Baujard Antoinette, *Beyond the Consent Dilemma in Libertarian Paternalism, a Normative Void*, *Homo Oeconomicus*, Accedo Verlag, 2015, pp. 301-305.

Bensoussan Alain, *Algorithmes Prédictifs et Protection des Données Personnelles*, Alain Bensoussan Avocats, 19 novembre 2015, disponible sur https://www.alain-bensoussan.com/algorithmes-predictifs-2/2015/11/19/ (consulté le 01/09/17).

Berrebi-Hoffmann Isabelle, Saint-Martin Arnaud, *Vie Privée et Démocratie, un Couple en Tension*, Socio, 7, 2016, pp. 7-23.

Bioy Xavier. *Le Libre Développement de la Personnalité en Droit Constitutionnel Essai de Comparaison (Allemagne, Espagne, France, Italie, Suisse),* Revue internationale de droit comparé. Vol. 55 N°1. Janvier-mars 2003, pp. 123-147.

Burket H, *Dualities of Privacy – An Introduction to « Personal Data Protection and Fundamental Rights »*, dans M.V. Perez, A. Palazzi, Y. Poullet (eds), Privacy – New Visions, Cahier du Crid, n°31,2008, pp. 13-23.

Borking John, *Privacy Enhancing Technologies*, Based on a Joint Study in Netherlands and Ontario, 1995.

Caragliu Andrea, *Smart Cities in Europe*, Journal of Urban Technology, Volume 18, 2011, pp. 65-82.

Cazé-Gaillarde Nathalie, *Vie Privée (Atteintes à la)*, Répertoire de droit pénal et de procédure pénale, Dalloz, Octobre 2014.

Cédras Jean, *Le Solidarisme Contractuel en Doctrine et Devant la Cour de Cassation*, Site internet de la Cour de Cassation, disponible sur https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2003_37/deuxieme_partie_tudes_documents_40/tudes_diverses_43/doctrine_devant_6260.html (consulté le 01/09/17).

Charlot Patrick, *Péguy contre Jaurès : L'Affaire des Fiches et la Délation aux Droits de l'Homme*, Revue Française d'histoire des idées politiques, n°17, 1 semestre 2003, pp. 73-91.

Chazal Jean-Pascal, *La protection de la partie faible chez Josserand, ou la tentative de maintenir le compromis républicain*, Un ordre juridique Nouveau ? Dialogue avec Louis Josserand, dir. Dross William, Favario Thierry, Mare et Martin, 2014, pp. 227-244.

Chénedé Francois, *De l'Autonomie de la Volonté à la Justice Commutative, du Mythe à la Réalité*, Annuaire de l'Institut Michel Villey, 2012, 4, pp. 155-181.

Cordier François, *L'Atteinte à l'Intimité de la Vie Privée en Droit Pénal et les Médias*, Legicom, 4/1999, n°20, 1999, pp. 85-93.

De Mauro Andrea, Greco Marco, *What is big data ? A consensual definition and a review of key research topics*, AIP Conference Proceedings 2015, pp. 97-104.

Demeulenaere Pierre, *Les Difficultés de la Caractérisation de la Notion de Vie Privée d'un Point de Vie Sociologique*, La Protection de la Vie Privée dans la Société de l'Information, Chapitre 11, pp. 194-200.

Deleuze Gilles, *Post-Scriptum sur les Sociétés de Contrôle*, Pourparlers, Les Editions de Minuit, Paris, 1990, pp. 240-247.

Faghmous James H., Kumar Vipin, *A Big Data Guide to Understanding Climate Change: the Case for Theory-Guided Data Science*, Big Data, volume 2, issue 3, September 15, 2014, pp. 155-163.

Féral-Schuhl Christiane, *Peut-on Protéger la Vie privée à l'Heure du Numérique ?,* publié le 27 avril 2015, disponible sur http://www.feral-avocats.com/fr/publication/peut-on-proteger-la-vie-privee-a-lheure-du-numerique/ (consulté le 01/09/17).

Flueckiger Alexandre, *L'Autodétermination en Matière de Données Personnelles : un Droit (plus si) Fondamental à l'Ere Digitale ou Nouveau Droit de Propriété ?*, Pratique juridique actuelle, 2013, vol. 22, pp. 837-864.

Forest David, *La Régulation des Algorithmes, entre Ethique et Droit*, Lamy Droit de l'Immatériel, 2014.

Gandomi Amir, Haider Murtaza, *Beyond the hype : Big data concepts, methods and analytics*, International Journal of Information Management, Volume 35, issue 2. April 2015, pp. 137-144.

Goldberg Ian, Wagner David, Brewer Eric, *Privacy-Enhancing technologies for the Internet*, Proceedings IEEE COMPCON 97, Digest of Papers, San Jose, CA, USA, 1997, pp. 103-109.

Chourabi H. et al., *Understanding Smart Cities: An Integrative Framework,* 2012 45th Hawaii International Conference on System Sciences, Maui, HI, 2012, pp. 2289-2297.

Hoffman A. David, *FTC Staff Preliminary Report on Protecting Consumer Privacy*, File n°P095416, January 26 2011, disponible sur https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00246-57451.pdf (consulté le 01/04/17).

Hollerith Herman, *The Electrical Tabulating Machine,* Journal of the Royal Statistical Society, Vol. 57, n°4, December 1894, pp. 678-689.

Jamin Christophe, *Relire Labbé et ses Lecteurs*, Archive de la Philosophie du Droit, 37, 1992, pp. 247-267.

Kahneman Daniel, Amos Tversky, *Choices, Values and Frames*, American Psychologist, April 1984, pp. 341-350.

Lavenue Jean-Jacques, *Gouvernance des données et naissance du Monstre Doux,* in Bouhadana Irene, Gilles William, *Droit et gouvernance des données publiques et privées à l'ère du numérique,* Imodev, 2015, pp. 35-56.

Lavenue Jean-Jacques, *La Privacy By Design : Panacée ou cheval de Troie ?,* Revue de la Recherche Juridique, Droit Prospectif, 2013-1, pp. 59-73.

Lavenue Jean-Jacques, Codron Clémence, Desrumaux Nicolas, Hamerel Gaylord B., *Privacy By Design ou Privacy By Law*, Revue Droit international, Commerce, Innovation et Développement, n°2/2012, novembre 2012, Presses de l'Université de Bourgogne, pp. 77-104.

Lazaro Christophe, Le Metayer Daniel, *Le Consentement au Traitement des Données Personnelles : une Perspective Comparative sur l'Autonomie du Sujet*, Revue juridique Thémis de l'Université de Montréal, voi.48 n°3, 2015, pp. 765-815.

Lindon Raymond, *La Presse et la Vie Privée*, JCP, 1975, I, 1887.

Mao Qi-rong, Pan Xin-yu, Zhan Yong-zhao, Shen Xian-jun, *Using Kinect for real-time emotion recognition via facial expressions*, Frontiers of Information Technology & Engineering, 2015 16(6), 272-282p.

Martial-Braz Nathalie, *L'Extraterritorialité des Décisions des Autorités de Régulation : Gage d'Efficacité de la Protection des Données Personnelles en Europe,* Colloque : La coopération policière, douanière et judiciaire en Europe, Besançon, 24 septembre 2015.

Moritz Marcel, *Les Perquisitions en Ligne et la Surveillance d'Internet*, Revue Le Lamy Droit de l'Immatériel, n°41, 1er août 2008, pp. 52-62.

Mornington Alicia-Dorothy, *La Fiction du Consentement dans les Relations Asymétriques entre Employé et Employeur,* La langue du management et de l'économie à l'ère néo-libérale : formes sociales et littéraires, textes réunis par Corinne Grenouillet et Catherine Vuillermot-Febvet, Presses Universitaires de Strasbourg, coll. Formes et Savoirs, 2015.

Murdoch Travis, Detsky Allan, *The Inevitable Application of Big Data to Health Care*, JAMA, 2013, 309(13), pp. 1351-1352.

Mathieu Bertrand, *Droit Constitutionnel Civil*, Jurisclasseur Administratif, 1997, Fasc. 1449, 1990.

McDonald Aleecia, Cranor Lorrie Faith, *The Cost of Reading Privacy Policies*, I/S: A journal of Law and Policy for the Information Society, 2008.

Ochoa Nicolas, *Pour en Finir avec l'Idée d'un Droit de Propriété sur ses Données Personnelles : Ce que Cache Véritablement le Principe de Libre Disposition*, RFDA, 2015, n°6, pp. 1157-1173.

Perray Romain, *Jurisclasseur Administratif*, Fasc. 274-20, 18 mai 2016.

Poullet Yves, Rouvroy Antoinette, *Le Droit à l'Autodétermination Informationnelle et la valeur du développement personnel. Une Réévaluation de l'importance de la vie privée pour la démocratie*, Etat de Droit et virtualité, Ed. Karim Benyekhlef & Pierre Trudel, Montréal: thémis, 2009, pp. 157-222.

Provost Foster, Fawcett Tom, *Data science and its relationship to Big Data and Data-Driven decision making*, Big Data vol. 1, Issue 1, February 13, 213, pp. 51-59.

Solove, Daniel J., Privacy *Self-Management and the Consent Dilemma*, Harvard Law Review n°1880, 2013, pp. 141-165.

Suart Ward Jonathan, Barker Adam, *Undefined by Data: A survey of Big Data Definitions*, University of St Andrews, 20 September 2013.

Thuillier Guy, *Morale et Politique : Péguy et l'Affaire des Fiches en 1905*, La Revue administrative, 43e Année, n°256, Juillet-Août 1990, pp. 310-316.

Tversky Amos, Kahneman Daniel, *The Framing of Decision and the Psychology of Choice*, Science, New Series, Vol. 211, N° 4481, January 30 1981, pp. 453-457.

Vallet Caroline, *Le Dévoilement de la Vie Privée sur les Sites de Réseau Social, des Changements Significatifs*, Droit et Société n°80, 2012/1, pp. 163-188.

Wang Yang, Kobsa Alfred, *Privacy-Enhancing Technologies*, Handbook of research on social and organizational liabilities in information security, IGI Global, 2009, pp. 203-227.

Warren Samuel, Brandeis Louis, *The Right to Privacy*, Harvard Law Review, vol. IV, December 15, 1890, pp. 193-220.

Zanfir Gabriela, *Forgetting about consent: why the focus should be on suitable safeguards in data protection law*, University of Craiova, May 2013.

2 - Articles de Vulgarisation Scientifique

Applebaum Jacob, Gibson Aaron et. al., *Inside the NSA's war on internet security*, Spiegle.de, 26 decembre 2014, disponible sur http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html (consulté le 01/09/17).

Bathelot Bertrand, *Définition: Plugins sociaux*, Définitions Marketings, Encyclopédie illustrée du marketing, 28 juillet 2015, disponible sur http://www.definitions-marketing.com/definition/plugins-sociaux/ (consulté le 01/09/2017).

Bathelot Bertrand, *Définition Yield Management*, Définition Marketing, l'Encyclopédie illustrée du marketing, 16 Mai 2015, disponible sur http://www.definitions-marketing.com/definition/yield-management/ (consulté le 01/09/2017).

Bathelot Bertrand, *Définition: Data Broker*, Définition Marketing, Encyclopédie illustrée du marketing, 22 mars 2017, disponible sur https://www.definitions-marketing.com/definition/data-broker/ (consulté le 01/09/17).

Calixte Laurent, *Billets d'avions : comment échapper à l'IP tracking des compagnies aériennes*, Challenges, 12 juin 2013, disponible sur http://www.challenges.fr/entreprise/20130612.CHA0739/billet-d-avions-comment-echapper-a-l-ip-tracking-des-compagnies-aeriennes.html (consulté le 01/09/2017).

Cappelli Patrick, *Les Nudges, Force de persuasion*, 19 janvier 2014, disponible sur http://www.liberation.fr/futurs/2014/01/19/les-nudges-force-de-persuasion_973983 (consulté le 01/09/17).

Dasquié Guillaume, *Le Business Secret des Data-Brokers*, GQ, 25 janvier 2016, disponible sur http://www.gqmagazine.fr/pop-culture/gq-enquete/articles/le-business-secret-des-data-brokers/29845 (consulté le 01/09/17).

Eudes Yves, *Hackers d'Etat, Enquête sur ces sociétés de sécurité offensive spécialisées dans la découverte de failles informatiques, qui vendent leurs trouvailles à des organismes officiels*, Le Monde, 19 février 2013, disponible sur http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html (consulté le 01/09/17).

Gandillot Thierry, *Holocauste : Les listes IBM,* L'express, 15 février 2001, disponible sur http://www.lexpress.fr/informations/holocauste-les-listes-ibm_641323.html (consulté le 01/09/17).

Gayat Pascal, *Blocage des Cookies, Quels Enjeux pour le Marketing à la Performance ?*, Journal du net, 29 mars 2013, disponible sur http://www.journaldunet.com/ebusiness/expert/53814/blocage-des-cookies--quels-enjeux-pour-le-marketing-a-la-performance.shtml (consulté le 01/09/19).

Greenwald Glenn, *NSA Collecting Phone Records of Millions of Verizon Customers,* The Guardian, 6 juin 2013.

Hourdeaux Jérome, *Gendarmes et Industriels Imaginent un Nouveau Logiciel pour Prédire le Crime*, Médiapart, 25 mai 2015, disponible sur https://www.mediapart.fr/journal/france/250515/gendarmes-et-industriels-imaginent-un-nouveau-logiciel-pour-predire-le-crime?onglet=full (consulté le 01/09/17).

Jobs Steve, *Thoughts on Flash*, April 2010, Apple.com, disponible sur https://www.apple.com/hotnews/thoughts-on-flash/ (consulté le 01/09/17).

Keegan Jon, *Blue Feed, Red Feed*, Wall Street Journal, 18 May 2016, disponible sur http://graphics.wsj.com/blue-feed-red-feed/#/health-care (consulté le 01/09/17).

Menn Joseph, *Social Networks can Scan for Sexual Predators, with uneven results*, Reuters, 12 July 2012, disponible sur http://www.reuters.com/article/us-usa-internet-predators-idUSBRE86B05G20120712 (consulté le 01/09/17).

Ribeiro John, *Google Part en Guerre Contre Flash avec HTML5*, Le Monde, disponible sur http://www.lemondeinformatique.fr/actualites/lire-google-part-en-guerre-contre-flash-avec-html5-64824.html (consulté le 01/04/17).

Sender Elena, *Lire dans les Pensées ? Les Neurosciences Y Sont Presque*, Sciences et Avenir, 19 juin 2015, disponible sur https://www.sciencesetavenir.fr/sante/lire-dans-les-pensees-les-neurosciences-y-sont-presque_29175 (consulté le 01/02/17).

Spiegle Online, *Sorge vor Kartell : Maas hatte gerne, dass Google geheime Suchformel offenlegt*, Spiegle Online, 16.09.2014, http://www.spiegel.de/wirtschaft/unternehmen/google-heiko-maas-fordert-offenlegung-von-algorithmus-a-991799.html (consulté le 01/09/17).

Untersinger Martin, *En trois ans, qu'a-t-on appris des documents Snowden ?,* Le Monde, 17 décembre 2016.

World Economic Forum, *Unlocking the Value of Personal Data: From Collection to Usage*, Prepared in collaboration with the Boston Consulting Group, February 2013.

3 - Articles d'Actualité

20 Minutes avec AFP, *Menace terroriste : Israël affirme avoir créé une technique pour identifier les « loups solitaires »*, 20 Minutes, 28 juillet 2016, disponible sur http://www.20minutes.fr/societe/1901367-20160728-menace-terroriste-israel-affirme-avoir-cree-technique-identifier-loups-solitaires (consulté le 01/09/17).

AFP, *Jean-Luc Lahaye condamné à un an de prison avec sursis*, Le Figaro, 18 mai 2015, disponible sur http://www.lefigaro.fr/musique/2015/05/18/03006-20150518ARTFIG00101-proces-de-jean-luc-layahe-le-verdict-tombe-ce-lundi.php (Consulté le 01/09/2017).

Arrington Michael, Facebook Launches Facebook Platform, TechCrunch*, 24 Mai 2007, disponible sur https://techcrunch.com/2007/05/24/facebook-launches-facebook-platform-they-are-the-anti-myspace/ (Consulté le 01/09/17)*.

Boucher Philippe, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.

Challenges.fr, *Facebook pulvérise ses bénéfices et son audience*, 28 janvier 2016, disponible sur http://www.challenges.fr/internet/20160128.CHA4405/facebook-pulverise-ses-benefices-et-son-audience.html (consulté le 01/09/2017).

Clapaud Alain, *ROI, Croisement des données, volatilité des clients : Carrefour monétise ses Datas*, La revue du Digital, disponible sur http://www.larevuedudigital.com/roi-croisement-des-donnees-volatilite-des-clients-big-data-tout-sur-la-strategie-de-carrefour-medias/ (consulté le 01/09/17).

Eustache Sophie, *Données personnelles : ¾ des Français ne font pas confiance aux applis mobiles*, L'Usine Digitale, 21 avril 2016, disponible sur http://www.usine-digitale.fr/article/donnees-personnelles-3-4-des-francais-ne-font-pas-confiance-aux-applis-mobiles.N387806 (consulté le 01/09/17).

Gavois Sébastien, *Yahoo annonce le vol de données de plus d'un milliard de compte*, Next Impact, 15 décembre 2016, disponible sur https://www.nextinpact.com/news/102530-yahoo-annonce-vol-donnees-plus-dun-milliard-comptes.htm (consulté le 01/09/17).

Génération NT*, Blizzard mise sur le streaming sur Facebook,* Génération NT, 7 juin 2016, disponible sur https://www.generation-nt.com/blizzard-accord-streaming-facebook-actualite-1929576.html (consulté le 01/09/17).

Girard Laurence, *Le retour des écrans publicitaires dans le métro*, Le Monde, 29 avril 2010.

Le Monde.fr, *Bernard Cazeneuve veut « une initiative Européenne » contre le chiffrement*, Le Monde, 12 août 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/08/12/bernard-cazeneuve-veut-une-initiative-europeenne-contre-le-chiffrement_4981741_4408996.html (consulté le 01/09/17).

Le Monde.fr, *Les principaux vols de donnée personnelles depuis 2013*, Le Monde, 29 septembre 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/09/23/les-principaux-vols-de-donnees-personnelles-depuis-2013_5002435_4408996.html (consulté le 01/09/17).

Le Monde.fr, *Publicités électorales russes : Facebook détaille ce qu'il a remis au Congrès américain*, 3 octobre 2017, disponible sur http://abonnes.lemonde.fr/pixels/article/2017/10/03/publicites-electorales-russes-facebook-detaille-ce-qu-il-a-remis-au-congres-americain_5195456_4408996.html (consulté le 01/09/19)

Next-impact, *Biométrie : la RATP veut faire payer à la face pour supprimer les queues*, Next Impact, 22 mai 2013, disponible sur https://www.nextinpact.com/news/79897-biometrie-ratp-veut-faire-payer-a-face-pour-supprimer-queues.htm (consulté le 01/09/17).

Next-impact, *La RATP abandonne son projet de péage par reconnaissance faciale,* Next Impact, 22 mai 2013, article disponible sur https://www.nextinpact.com/news/79901-la-ratp-abandonne-son-projet-peage-par-reconnaissance-faciale.htm (consulté le 01/09/17).

Nick O'Neill, *50 000 websites add Facebook's Like button and social plugins in first week*, Adweek, 28 April 2010, disponible sur http://www.adweek.com/digital/50000-websites-add-facebooks-like-button-and-social-plugins-in-first-week/ (consulté le 01/09/17).

O'Ryan Johnson, *FBI wants Iphone unlocked in Boston gang case*, Boston Herald, 15 mars 2016, disponible sur http://www.bostonherald.com/news/local_coverage/2016/03/fbi_wants_iphone_unlocked_in_boston_gang_case (consulté le 01/09/17).

Ouest France, *Terrorisme : la messagerie Telegram donne du fil à retordre aux policiers*, Ouest France, 16 septembre 2016, disponible sur http://www.ouest-france.fr/terrorisme/terrorisme-la-messagerie-telegram-donne-du-fil-retordre-aux-policiers-4495497 (consulté le 01/09/17).

Perez Evan, Hume Tim, *Apple Opposes judge's order to hack San Bernardino shooter's,* CNN, disponible sur http://edition.cnn.com/2016/02/16/us/san-bernardino-shooter-phone-apple/index.html (consulté le 01/09/17).

Puiatti Sonia, *Seulement 37% des Français sont confiants dans l'usage d'Internet*, EcommerceMag, 24 octobre 2016, disponible sur http://www.ecommercemag.fr/Thematique/indicateurs-1010/Breves/Seulement-Fran-ais-sont-confiants-dans-usage-Internet-309918.htm (consulté le 01/09/17).

Reitman Rainey, *White House, Google and Other Advertising Companies Commit to Supporting Do Not Track*, Electronic Frontier Foundation, 23 February 2012, disponible sur https://www.eff.org/fr/deeplinks/2012/02/white-house-google-and-other-advertising-companies-commit-supporting-do-not-track (consulté le 01/09/17).

Statista, The Statistics Portal, *Number of monthly active Facebook users worldwide as of 2nd quarter 2016 (in millions)*, Statista, Disponible sur http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (consulté le 01/09/17).

Szadkowski Michel, Leloup Damien, *Facebook, faiseur de rois de l'élection Américaine ?,* Le Monde, 14 novembre 2016, disponible sur http://www.lemonde.fr/pixels/article/2016/11/14/facebook-faiseur-de-rois-de-l-election-americaine_5030959_4408996.html (consulté le 01/09/17).

Tual Morgane, *Facebook passe la barre des deux milliards d'utilisateurs*, Le Monde, 27 juin 2017, disponible sur http://www.lemonde.fr/pixels/article/2017/06/27/facebook-passe-la-barre-des-2-milliards-d-utilisateurs_5152063_4408996.html (consulté le 01/09/17).

Untersinger Martin, *Suicides, démission, chantage : les conséquences tragiques du piratage du site de rencontres Ashley Madison*, Le Monde, 10 décembre 2015, disponible sur http://www.lemonde.fr/pixels/article/2015/12/10/suicides-demission-chantage-les-consequences-tragiques-du-piratage-du-site-de-rencontres-ashley-madison_4828391_4408996.html (consulté le 01/09/17).

Waters Darren, *EC starts legal action over Phorm*, BBC News website, disponible sur http://news.bbc.co.uk/2/hi/technology/7998009.stm (Consulté le 01/09/17).

Wavestone, *Smart Cities et mobilité : la France en pointe sur le marché stratégique des métros automatiques*, Communiqué de Presse, 26 avril 2017, disponible sur http://wellcom.fr/presse/wavestone/2017/04/smart-cities-et-mobilite-france-en-pointe-sur-marche-strategique-des-metros-automatiques/ (consulté le 01/09/17).

We Are Social, *Digital, Social and Mobile* 2015, WeAreSocial, disponible sur http://wearesocial.com/fr/etudes/digital-social-mobile-les-chiffres-2015 (consulté le 01/09/2017).

Zephoria, *Top 20 valuable Facebook Statistics,* Juillet 2016, disponible sur https://zephoria.com/top-15-valuable-facebook-statistics/ (consulté le 01/09/17).

III - Thèses et Rapports Spécialisés

1 - Thèses

Ochoa Nicolas, *Le droit des données personnelles, une police administrative spéciale*, Droit. Université Paris 1 Panthéon-Sorbonne, 2014, HAL Id : Tel-01340600.

Gutmann Daniel, *Le sentiment d'identité,* L.G.D.J., 536 p.

Zwolinska Monika, *Sécurité et libertés fondamentales des communications électroniques en droit Français, Européen et International*, Droit, Université Sophia Antipolis, 4 décembre 2014, 584 p.

2 - Rapports

Adam Patricia, *Rapport n° 4573 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016*, Enregistré à la Présidence de l'Assemblée Nationale le 2 mars 2017.

Bas Philippe, *Rapport n°460 fait au nom de la commission des lois, au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du règlement et d'administration générale, sur le projet de loi, adopté par l'Assemblée nationale, après engagement de la procédure accélérée, relatif au renseignement et, sur la proposition de loi organique relative à la nomination du président de la commission nationale de contrôle des techniques de renseignement*, Déposé à l'Assemblée Nationale le 20 mai 2015.

Bonhomme François, Leconte Jean-Yves, *Rapport d'information n°788 fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur l'usage de la biométrie en France et en Europe*, Enregistré à la Présidence du Sénat le 13 juillet 2016.

Braun Gérard, *Rapport d'information n°402 fait au nom de la commission des finances, du contrôle budgétaire et des comptes économiques de la Nation sur l'administration électronique au service du citoyen*, Annexe au procès-verbal de la séance du 6 juillet 2004.

Chenot Bernard, Aydalot Maurice, Tricot Bernard et. al., *Rapport de la Commission de l'Informatique et des libertés*, Paris, 1975, 128 p.

Commission Nationale de Contrôle des Techniques de Renseignement, *1er rapport d'activité 2015-2016*, 2016.

Commission Nationale de l'Informatique et des Libertés, *Rapport d'activité 2016*, La Documentation Française. 2016.

Conseil d'Etat, *Etude annuelle 2014, Le numérique et les droits fondamentaux*, Doc. Fr, 2014, coll. Les rapports du Conseil d'Etat, septembre 2014.

Cour de Cassation, *Rapport 2010*, La Documentation Française, Paris, 2011.

Coutelle Catherine, *Rapport d'information n°3318 fait au nom de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes sur le projet de loi pour une République numérique*, Enregistré à la Présidence de l'Assemblée nationale le 15 décembre 2015.

Détraigne Yve, Escoffier Anne-Marie, *Rapport d'information n°441 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, Annexe au procès-verbal de la séance du 27 mai 2009.

Fagan Jeffrey, Braga Anthony et.al., *Final Report: An analysis of Race and Ethnicity Patterns in Boston Police Department Field Interrogation, Observation, Frisk, and/or Search Reports*, June 2015.

Féral-Schul Christiane, Paul Christian, *Rapport d'information n°3119 sur le droit et les libertés à l'âge du numérique*, Déposé à l'Assemblée Nationale le 8 octobre 2015.

Foyer Jean, *Rapport n°3125 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur le projet de loi n°2516 relatif à l'informatique et aux libertés par M. Foyer*, Assemblée Nationale, Annexe au procès-verbal de la séance du 4 octobre 1977.

Francillon Jacques, *Cybercriminalité : aspects de droit pénal international*, rapport présenté à l'association international de droit pénal, XIX congres international de droit pénal, 12 juin 2013.

Goujon Philippe, *Rapport n°3599 fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur la proposition de loi n°3471 adoptée par le Sénat, relative à la protection de l'identité*, enregistré à la présidence de l'Assemblée Nationale le 29 juin 2011.

Lecerf Jean-René, *Rapport d'information n°439 fait au nom de la commission des lois et de la mission d'information de la commission des lois*, Séant, Annexe au procès-verbal de la séance du 29 juin 2005.

McKinsey Global Institute, *Big Data: The next frontier for innovation, competition and productivity*, May 2011.

Nechvatal James et. al., *Report on the Development of the Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, U.S. Department of Commerce, 2 October 2000.

Observatoire National de la délinquance et des réponses pénales, *Rapport Annuel 2016 de l'ONDRP, La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet en 2015, novembre 2016.*

Truste/TNS Survey, *Consumers have false sense of security about online privacy, actions inconsistent with attitudes*, Rapport daté du 6 décembre 2006.

Trend Micro, *Rapport de sécurité pour le 1er trimestre 2016*, disponible sur http://www.trendmicro.fr/newsroom/pr/le-rapport-de-securite-de-trend-micro-pour-le-premier-semestre--met-en-avant-la-recrudescence-des-ransomware-et-des-arnaques-bec-business-email-compromise/index.html (consulté le 01/09/17).

Turk Alex, *Rapport n°218 fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, Annexe au procès-verbal de la séance du 19 mars 2003.

U.S. Department of Justice, Civil Rights Division, *Investigation of the Baltimore city police department*, August 10 2016.

IV – Communications, Avis et Déclarations Publiques

1 – Communications de l'ANSSI

Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI), *Stratégie nationale pour la sécurité du numérique*, 2015.

Agence Nationale de la Sécurité des Systèmes d'Informations, *Contrôle règlementaire de la cryptographie*, *Démarches à accomplir*, voir tableau de synthèse disponible sur www.ssi.gouv.fr (consulté le 01/07/17).

2 - Communications de la Commission Européenne

Commission Européenne, *Communication on the protection of individuals in relation to the processing of personal data in the Community and information security, Draft resolution of the representatives of the governments of the member states of the European Communities meeting within the Council*, COM/90/314 final, Brussels, 13 September 1990.

Commission Européenne, *Technologies renforçant la protection de la vie privée*, Mémo 07/159, Bruxelles, 2 mai 2007.

Commission Européenne**,** *Telecoms: Commission launches case against UK over privacy and personal data protection*, IP/09/570, Brussels, 14 April 2009.

Commission Européenne, *Une approche globale de la protection des données à caractère personnel dans l'union Européenne*, COM/2010/0609 final, Bruxelles, 4 novembre 2010.

Commission Européenne, Directorate General for Justice, *Take control of your personal data*, Luxembourg, Publications Office of the European Union, 2012.

Commission Européenne, *Communication de la Commission au Parlement Européen, au Conseil, au Comité Economique et Social Européen et au Comité des Régions, Protection de la vie privée dans un monde en réseau : un cadre européen relatif à la protection des données, adaptés aux défis du 21e siècle*, IP 2012/9, Bruxelles, le 25 janvier 2012.

Commission Européenne, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*, COM/2012/11 Final, Brussels, 25 January 2012.

Commission Européenne, *Communiqué de Presse*, IP/12/558, Bruxelles, 4 Juin 2012.

Commission Européenne, *Communication from the Commission to the European Parliament and the Council, on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM/2013/847 Final, Brussels, 27 November 2013.

Commission Européenne, *La Commission Européenne présente le paquet « bouclier de protection des données UE-Etats-Unis » : des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données*, IP/16/433, Bruxelles, 29 février 2015.

Commission Européenne, *Un marché unique numérique pour l'Europe : la Commission définit 16 initiatives pour en faire une réalité*, IP 15/4919, Bruxelles, 6 mai 2015.

Commission Européenne, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[First Reading],* Brussels, 15 December 2015.

Commission Européenne, *Communiqué de Presse*, IP/16/2016, Strasbourg, 2 février 2016.

Commission Européenne, *Mergers: Commission's alleges Facebook provided misleading information about WhatsApp takeover*, IP/16/4473, Brussels, 20 December 2016.

Commission Européenne, *Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/CE (Regulation on Privacy and Electronic Communications)*, COM/2017/10 Final, Brussels, 10 January 2017.

3 – Communications de la CNIL

Commission Nationale de l'Informatique et des Libertés, *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL Européennes*, 2 Août 2007.

Commission Nationale de l'Informatique et des Libertés*, Peer-to-Peer : la CNIL se tourne vers l'avenir*, 17 décembre 2007.

Commission Nationale de l'Informatique et des Libertés, *Pas de publicité via Bluetooth sans consentement préalable*, Communication du 12 novembre 2008.

Commission Nationale de l'Informatique et des Libertés, *La publicité ciblée en ligne,* Communication présentée en séance plénière le 5 février 2009.

Commission Nationale de l'Informatique et des Libertés, *Notion d'interconnexion*, Communication datée du 5 avril 2011, disponible sur https://www.cnil.fr/fr/comment-determiner-la-notion-dinterconnexion (Consulté le 01/09/2017)

Commission Nationale de l'Informatique et des Libertés, Note d'observation concernant la proposition de loi relative à la protection de l'identité, Examinée en séance plénière le 25 octobre 2011.

Commission Nationale de l'Informatique et des Libertés, *Guide : mesures pour traiter les risques sur les libertés et la vie privée*, Edition 2012.

Commission Nationale de l'Informatique et des Libertés, « *Recommandation sur les cookies : quelles obligations pour les responsables de sites, quels conseils pour les internautes ?* », 16 décembre 2013.

Commission Nationale de l'Informatique et des Libertés, *IP Tracking : conclusion de l'enquête conjointe menée par la CNIL et la DGCCRF,* 27 Janvier 2014.

Commission Nationale de l'Informatique et des Libertés, *Politique de confidentialité de Google : le G29 propose un pack de conformité*, 25 septembre 2014.

Commission Nationale de l'Informatique et des Libertés, *PIA : La méthode*, CNIL, Edition juin 2015.

Commission Nationale de l'Informatique et des Libertés, *Editeurs de sites pour enfants : n'oubliez pas vos obligations*, 2 septembre 2015.

Commission Nationale de l'Informatique et des Libertés, « *Exemple de Bandeau Cookies : comment recueillir valablement le consentement des internautes aux cookies et traceurs de votre site ou application web ?* », 30 décembre 2015, site internet de la CNIL, https://www.cnil.fr/fr/exemple-de-bandeau-cookie (consulté le 01/09/17).

Commission Nationale de l'Informatique et des Libertés, *La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de trois mois, à la loi informatique et libertés*, Communication datée du 9 février 2016, disponible sur https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi (consulté le 01/09/2017).

Commission Nationale de l'Informatique et des Libertés, *Vidéo dans les cellules de détention : l'avis de la CNIL*, 14 juin 2016, disponible sur https://www.cnil.fr/fr/video-dans-les-cellules-de-detention-lavis-de-la-cnil (consulté le 01/09/17).

Commission Nationale de l'Informatique et des libertés, *Règlement Européen : ce qui change pour les professionnel, Communication du 15 juin 2016*, disponible sur https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels (consulté le 01/09/17).

Commission Nationale de l'Informatique et des Libertés, *Biométrie : un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail*, 27 septembre 2016.

Commission Nationale de l'Informatique et des Libertés, *Consultation publique sur le règlement Européen, Synthèse des contributions sur la notification de violations, le consentement, le profilage*, Communication datée de mars 2017.

Commission Nationale de l'Informatique et des Libertés, « *Cookies & Traceurs : que dit la loi ?* », Non daté, disponible sur https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi (consulté le 01/09/17).

4 - Communications et Avis du G29 et du Contrôleur Européen

Contrôleur Européen de la protection des données, *Avis du contrôleur européen de la protection des données sur la communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions intitulée : « Une approche globale de la protection des données à caractère personnel dans l'Union Européenne* », 2011/C, Journal officiel de l'Union Européenne, 22 juin 2011, C 181/1.

Groupe de Travail « Article 29 » sur la protection des données, *Document de travail sur le respect de la vie privée sur internet, Une approche Européenne intégrée sur la protection des données en ligne*, adopté le 21 novembre 2000, 5063/00/FR/Final, WP 37

Groupe de Travail « Article 29 » sur la protection des données, *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, adopté le 13 septembre 2001, 5062/01/FR, WP 48.

Groupe de Travail « Article 29 » sur la protection des données, *Document de travail relatif à l'interprétation commune des dispositions de l'article 29, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995*, adopté le 25 novembre 2005, 2093-01/05/FR, WP 114.

Groupe de Travail « Article 29 » sur la protection des données, *Avis 5/2005 du groupe 29 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée*, adopté le 25 novembre 2005, 2130/05/FR, WP 115.

Groupe de Travail « Article 29 » sur la protection des données, *Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME)*, adopté le 15 février 2007, 00323/07/FR, WP 131.

Groupe de Travail « Article 29 » *sur le concept de données à caractère personnel*, adopté le 20 juin 2007, 0148/07/FR, WP 136.

Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*, adopté le 11 février 2009, 398/09/FR, WP 160.

Groupe de Travail « Article 29 » sur la protection des données, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »,* Adopté le 16 février 2010, 00264/10/FR, WP 169.

Groupe de Travail « Article 29 » sur la protection des données, *Avis 2/2010 sur la publicité comportementale en ligne*, adopté le 22 juin 2010, 00909/10/FR, WP 171.

Groupe de travail « Article 29 » sur la protection des données, *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12 January 2011, WP 180.

Groupe de Travail « Article 29 » sur la protection des données, A*vis 15/2011 sur la définition du consentement*, adopté le 13 juillet 2011, 01197/11/FR, WP 187.

Groupe de Travail « Article 29 » sur la protection des données, *Opinion 04/2012 on Cookie Consent Exemption*, adopted on 7 June 2012, 00879/12/EN WP 194.

Groupe de Travail « Article 29 » sur la protection des données, *Opinion 08/2012 providing further input on the data protection reform discussions*, Adopted on 5 October 2012, 01574/12/EN, WP 199.

Groupe de Travail « Article 29 » *opinion 03/2013 on purpose limitation*, adopted on 2 April 2013, 00569/13/EN, WP 203.

Groupe de Travail « Article 29 » sur la protection des données, *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, adopté le 9 avril 2014, 844/14/FR, WP 217.

Groupe de Travail « Article 29 » sur la protection des données*, Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, adopté le 16 septembre 2014, 1471/14/FR, WP 223.

Groupe de Travail « Article 29 » sur la protection des données, *Google Privacy Policy*, Ref. Ares (2014) 3113072, 23 septembre 2014.

Groupe de Travail « Article 29 » sur la protection des données, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*, Adopted on 22 September 2015, 2588/15/EN, WP 232.

Groupe de Travail « Article 29 » sur la protection des données *Opinion 01/2016 on the EU – U.S. Privacy Shield Draft adequacy decision, Adopted on 13 April 2016*, 16/EN, WP 238.

Groupe de Travail « Article 29 » sur la protection des données, *Guidelines on the right to data portability*, adopted on 13 December 2016, 16/EN, WP 242.

5 – Autres Communications

Ballestrazzi Mireille, propos recueillies par Sylvain Rolland, *La Cybercriminalité est la nouvelle menace du XXIeme siècle*, La tribune, 26 juillet 2015, disponible sur http://www.latribune.fr/technos-medias/internet/la-cybercriminalite-est-la-nouvelle-menace-du-xxie-siecle-485152.html (consulté le 01/09/17).

Cazeneuve Bernard, *Déclaration publique lors du compte rendu intégral de la Première séance du Mardi 14 Avril 2015*, Assemblée Nationale, 14 avril 2015.

Cloud Select Industry Group, *Data Protection Code of Conduct for Cloud Service Provider*, 19 January 2015.

Comité Directeur pour les Droits de l'Homme, Groupe de rédaction sur les droits de l'homme dans les sociétés culturellement diverses, *Déclarations publiques lors du Projet de Compilation des normes du Conseil de l'Europe relatives aux principes de liberté de pensée, de conscience et de religion et liens avec d'autres droits de l'homme*, Conseil de l'Europe, Strasbourg, 11 Mars 2015.

Commission Nationale de l'Informatique et des Libertés, *Lettre adressée à Google Inc,* Paris, 27 février 2012.

Conseil National du Numérique, *Rapport Ambition Numérique : Pour une politique Française et Européenne de la transition numérique*, Rapport remis au Premier Ministre, Juin 2015.

Conseil National du Numérique, *Tribune : chiffrement et lutte contre le terrorisme, attention à ne pas se tromper de cible,* disponible sur https://cnnumerique.fr/tribune-chiffrement/ (consulté le 01/09/17).

Damasio Alain, Propos recueillies dans : Fradin Andréa, *L'auteur de SF Alain Damasio dissèque la société de contrôle « C'est pas Big Brother c'est Big Mother »*, Les Inrocks, 25 novembre 2013, disponible sur http://www.lesinrocks.com/2013/11/25/medias/lauteur-sf-alain-damasio-disseque-societe-controle-cest-pas-big-brother-cest-big-mother-11447605/ (consulté le 01/09/2017).

Falque-Pierrotin Isabelle, *Déclaration publique en présence de la Commission des lois*, 14 décembre 2011.

Hustinx Peter, Communication, *Respect de la vie privée dès la conception (Privacy by Design): le séminaire définitif*, Madrid, 2 nov. 2009, disponible sur http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf (consulté le 01/09/17).

Kroes Neelie, *Declaration publique à occasion de l'EIT Foundation Annual Innovation Forum: The Big Data Revolution*, Bruxelles, 26 mars 2013.

La Quadrature du Net, *Données personnelles et vie privée : la Quadrature du net répond à la Commission européenne*, Paris, 22 juin 2016.

Mallet-Poujol Nathalie, propos retranscrits dans Commission Nationale de l'Informatique et des Libertés, *Cahiers IP, Innovation et prospective n°1, Vie privée à l'horizon 2020 : Paroles d'experts,* 30 novembre 2012.

Meglena Kuneva, *Déclaration publique lors de la Roundtable on Online Data Collection, Targeting and Profiling*, Brussels, 31 March 2009.

Organisation de Coopération et de Développement Economiques, *Manuel d'Oslo*, *Principes directeurs pour le recueil et l'interprétation des données sur l'innovation*, 3eme édition, 2005.

Perrot Patrick, déclaration recueillie par Molinié William, *Viols, agressions, cambriolages : le nouvel algorithme des gendarmes pour prédire le crime*, 20 minutes, 21 mai 2015.

Reeding Viviane, Déclaration *publique: The EU Data Protection Reform 2012 : Making Europe The Standard Setter For Modern Data Protection Rules In the Digital Age lors de l'Innovation Conference Digital, Life, Design*, Munich, 22 January 2012.

Services du Premier Ministre, *France numérique 2012 -2020, Bilan et Perspectives,* Paris, Novembre 2011.

Therrien Daniel, Privacy Commissioner of Canada, *Speak recorded at the Privacy & Laws & Business 29th Annual Internal Conference*, Cambridge, 2-6 July 2016.

Shwartz Ari, Sherry Linda, Cooper Mark et al. Message to Donald S. Clark, Secretary of the Federal Trade Commission, *In advance of the FTC Town Hall, "Ehaviorial Advertising: Tracking, Targeting, and Technology",* to be held November 1-2, 2007 in Washington DC. Center for Democracy & technology.

The White House, *Communication:* C*onsumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy*, Washington, February 2012.

V - Références Normatives

1 – Textes et décisions d'origine nationale

1) Décisions constitutionnelles

Conseil Constitutionnel, 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*, Rec. p. 29, Journal officiel du 18 juillet 1971, p. 7114.

Conseil Constitutionnel, Décision n° 76-87 L, 3 mars 1976, Rec. p. 49.

Conseil Constitutionnel, Décision n° 83-164 DC du 29 décembre 1983, *Loi de finances pour 1984*, Rec. p. 67 - Journal officiel du 30 décembre 1983, p. 3871.

Conseil Constitutionnel, Décision n° 88-244 DC du 20 juillet 1988, *Loi portant amnistie*, Rec. p. 119 - Journal officiel du 21 juillet 1988, p. 9448.

Conseil Constitutionnel, Décision n° 94-352 DC du 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 - Journal officiel du 21 janvier 1995, p. 1154.

Conseil Constitutionnel, Décision n°96-377 DC du 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 - Journal officiel du 23 juillet 1996, p. 11108.

Conseil Constitutionnel, Décision n° 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, Rec. p. 100 - Journal officiel du 28 juillet 1999, p. 11250.

Conseil Constitutionnel, Décision n° 2003-484 DC du 20 novembre 2003, *Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité*, Rec. p. 438 - Journal officiel du 27 novembre 2003, p. 20154

Conseil Constitutionnel, Décision n° 2008-562 DC du 21 février 2008, *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*, Rec. p. 89 – Journal officiel du 26 février 2008, p. 3272, texte n°2.

Conseil Constitutionnel, Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, Rec. p. 158, Journal officiel du 28 mars 2012, p. 5607.

Conseil Constitutionnel, Décision n° 2014-693 DC du 25 mars 2014, *Loi relative à la géolocalisation*, JORF du 29 mars 2014, p. 6125, texte n° 2.

Conseil Constitutionnel, Décision n°2015-713 du 23 juillet 2015, *Loi relative au renseignement*, Journal officiel n°0171 du 26 juillet 2015, p. 12751, texte n°4.

Conseil Constitutionnel, Décision n°2016-590-QPC du 21 octobre 2016, *La Quadrature du Net et autres*, Journal officiel n°0248 du 23 octobre 2016, texte n°37.

2) Textes de valeur législative

Loi du 22 avril 1905, *portant fixation du budget des dépenses et des recettes de l'exercice 1905*, Recueil Duvergier, p. 268.

Loi du 9 décembre 1905, *concernant la séparation des Eglises et de l'Etat*, JORF du 11 décembre 1905, p. 7205.

Loi n°51-711 du 7 juin 1951, *sur l'obligation, la coordination et le secret en matière de statistiques*, JORF du 8 juin 1951, p. 6013.

Loi n°70-539 du 24 juin 1970, *sur la centralisation de la documentation relative à la circulation routière*, JORF du 25 juin 1970, p. 5963.

Loi °70-643 du 17 juillet 1970*, tendant à renforcer la garantie des droits individuels des citoyens*, JORF du 19 juillet 1970 p. 6751.

Loi n° 78-17 du 6 janvier 1978, *relative à l'informatique, aux fichiers et aux libertés,* JORF du 7 janvier 1978, p. 227.

Loi n°88-19 du 5 janvier 1988, *relative à la fraude informatique*, JORF du 6 janvier 1988, p. 231.

Loi n°91-646 du 10 juillet 1991, *relative au secret des correspondances émises par la voie des télécommunications*, JORF n° 106 du 13 juillet 1991, p. 9167.

Loi n° 93-1417 du 30 décembre 1993, *portant diverses dispositions relatives à la maitrise de l'immigration et modifiant le code civil,* JORF n°1 du 1 janvier 1994, p. 11.

Loi n°94-653 du 29 juillet 1994, *relative au corps humain*, JORF n°175 du 30 juillet 1994, p. 11056.

Loi n°2000-230 du 13 mars 2000, *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*, JORF n°62 du 14 mars 2000 p. 3968.

Loi n°2002-1094 du 29 août 2002, *d'orientation et de programmation pour la sécurité intérieure*, JORF du 30 août 2002, p. 14398, texte n°1.

Loi n°2004-575 du 21 juin 2004, *pour la confiance dans l'économie numérique*, JORF n°0142 du 22 juin 2004, p. 11168, texte n°2.

Loi n°2004-800 du 6 août 2004, *relative à la bioéthique*, JORF n°182 du 7 août 2004, p. 14040, texte n°1.

Loi n°2008-1350 du 19 décembre 2008, *relative à la législation funéraire*, JORF n°0296 du 20 décembre 2008, p. 19538, texte n°1.

Loi n° 2011-267 du 14 mars 2011, *d'orientation et de programmation pour la performance de la sécurité intérieure*, JORF n°0062 du 15 mars 2011, p. 4582, texte n°2.

Texte adopté n°883, Petite loi, Session ordinaire de 2011-2012, 6 mars 2012, sur la proposition de loi relative à la protection de l'identité.

Loi n°2012-410 du 27 mars 2012, *relative à la protection de l'identité*, JORF n°0075 du 28 mars 2012 p. 5604, texte n°2.

Loi n°2013-1168 du 18 décembre 2013, *relative à la programmation militaire pour les années 2014-2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, JORF n°0294 du 19 décembre 2013 p. 20570, texte n°1.

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, p. 19162.

Loi n°2015-912 du 24 juillet 2015, *relative au renseignement*, JORF n°0171 du 26 juillet 2015 p. 12735, texte n°2.

Loi n°2016-41 du 26 janvier 2016, *de modernisation de notre système de santé*, JORF n°0022 du 27 janvier 2016, texte n°1.

Loi n°2016-737 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, texte n°1.

Loi n°2016-987 du 21 juillet 2016, *prorogeant l'application de la loi n°55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste*, JORF n°1069 du 22 juillet 2016, texte n°2.

Loi n°2016-1321 du 7 octobre 2016, *pour une République numérique*, JORF n°0235 du 8 octobre 2016, texte n°1.

3) Textes de valeur infra-législative

Décret n°2001-272 du 30 mars *2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique*, JORF n°0077 du 31 mars 2001, p. 5070.

Décret n°2007-663 du 2 mai 2007 *pris en application des articles 30,31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relative aux moyens et aux prestations de cryptologie*, JORF n°104 du 4 mai 2007, p7865, texte n°1.

Décret n°2007-1145 du 30 juillet 2007 *portant création d'un traitement automatisé de données à caractère personnel dénommé "système de transmission d'interception judiciaires"*, JORF n°175 du 31 juillet 2007, p12862, texte n°23.

Décret n°2008-426 du 30 avril 2008 *modifiant le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques*, JORF n°0105 du 4 mai 2008 p7446, texte n°4.

Décret n°2011-219 du 25 février 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, JORF n°0050 du 1 mars 2011, p3643, texte n°32.

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, texte n°18.

Décret n°2017-173 du 13 février 2017 *précisant les modalités d'information des candidats à l'assurance-emprunteur lorsqu'ils présentent du fait de leur état de santé ou de leur handicap un risque aggravé*, JORF n°0038 du 14 février 2017, texte n°8.

Ordonnance n°2011-1012 du 24 août 2011 *relative aux communications électroniques*, JORF n°0197 du 26 août 2011 page 14473 texte n°49.

Ordonnance n°2017-31 du 12 janvier 2017 *de mise en cohérence des textes au regard des dispositions de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé,* JORF n°0011 du 13 janvier 2017, texte n°25.

4) Décisions des juridictions administratives

CE, 13 décembre 1999, *Caisse de crédit mutuel de Bain-Tresboeuf*, n° 197060, Rec. p. 397.

CE, 18 mars 2005, *Syndicat national de défense de l'exercice libéral de la médecine à l'hôpital*, n°238206, Rec. 49.

CE, 23 mai 2007, *SACEM*, n°288149, Inédit au Rec.

CE, 30 décembre 2009, *Association SOS Racisme, GISTI et autres*, n° 312051, Rec. p. 538.

CE, 16 avril 2010, *Association Inter-LGBT*, n°320196, Rec. p. 146.

CE, 12 mars 2014, *Pages Jaunes Groupe*, n°353193, Mentionné dans les tables du Recueil Lebon, ECLI:FR:CESSR:2014:353193.20140312.

CE, 11 mars 2015, *TUTO4PC*, n°368624, Mentionné dans les tables du Recueil Lebon, ECLI : FR : CESSR : 2015 :36862.20150311.

5) Décisions des juridictions judiciaires

T. civ. Nantes, 6 janvier 1956, Gaz. Pal. 1956, 1, 61.

TGI. Paris, 17eme chambre, Chambre de la presse, Jugement du 2 novembre 2000.

Cass. Crim, 31 janvier 1914, S, 1916, 1, p. 59.

CA. Paris, 7eme chambre, 15 mai 1970.

Cass. Civ., 26 Novembre 1975, n°74-10034, Bull. 1975, II, n°314, p. 289.

Cass. Com., 20 mai 1980, n°78-10833, Bull. Com. IV, n°212.

Cass. Soc., 8 novembre 1984, n°82-14816, Bull. Soc. 1984, V, n°423.

CA. Montpellier, 17eme ch, sect. D, 9 avril 1987, JCP, ed. G., II, n°20984.

Cass. Civ. 1re, 13 avril 1988, n°86-15524, Bull. Civ. 1988, I, n°98, p. 67.

Cass. Civ. 11 octobre 1988, n°86-12832, Bull. Civ. 1988, n°280, p. 192.

TGI. Paris, 30 novembre 1988.

Cass. Civ. 1re, 23 octobre 1990, n°89-13.163, Bull. Civ. 1990, I, n°222, p. 158.

TGI. Paris, 22 avril 1992.

CA. Douai, 7 octobre 1992.

CA. Paris, 18 octobre 1992.

Cass. Ass. Plén. 11 décembre 1992, n°91-11.900, Bull. civ. 1992 A.P. n°13 p. 27

TGI. Paris 15 décembre 1993.

CA. Paris, 5 avril 1994, D. 1994, IR, p. 130.

Cass. Com., 21 mars 1995, n°93-12.383, Bull. Com. 1995, IV, n°92, p. 82.

Cass. Crim, 22 janvier 1997, n°95-81186, Bull. Crim, 1997, n°31 p.83.

Cass. Com., 7 octobre 1997, n°95-30146, Bull. Com. IV, n°247, p. 215.

CA. Paris, 5 décembre 1997, D. 1998, IR 32, Gaz. Pal. 1998.1, somm. 234.

Cass. Crim, 20 octobre 1998, n°97-84621, Bull. Crim, 1998, n°264, p. 765.

TGI. Nanterre, Section C, 27 octobre 1998.

TI. Puteaux, 28 septembre 1999.

Trib. Corr. Paris, 13eme ch, 25 février 2000.

CA. Paris, 12eme ch, 30 octobre 2002.

Cass. Civ., 25 février 2004, n°02-18081, Bull. civ. 2004, III, n°41, p.729.

Cass. Civ. 2e, 10 mars 2004, n°01-15322, Bull. Civ. 2004, n°117, p. 97.

T. Corr. Nanterre, 4 juin 2004.

Cass. Crim., 1 septembre 2005, n°05-84.061, Bull. Crim. n°139, D. 2006, p. 2836.

TGI. Paris, 1ere ch., 4 avril 2006.

Cass. Civ., 11 décembre 2008, n°07-19494, Bull. Civ. 2008, I, n°282.

Cass. Soc., 13 janvier 2009, n°07-43282, Bull. Soc. 2009, V, n°3.

Cass. Crim., 30 novembre 2011, n°10-81749, Bull. Crim. 2011, n°243.

CA. Rennes, 17 janvier 2012, Répertoire Général n°10/07/599, arrêt n°15.

Cass. Civ., 4 mai 2012, n°10-27208, Gaz. Pal. 17 mai 2012, n°138, p. 13.

Cass. Civ., 19 septembre 2012, n°10-12.024, AJDI 2012, p. 754.

Cass. Com., 25 juin 2013, n°12-17037, Bull. Com. 2013, IV, n°108.

Cass. Crim., 27 mai 2014, n°13-80849, Bull. Crim. 2014, n°137**.**

Cass. Civ 1re, 15 janvier 2015, n°14-12200, non publié au bulletin.

CA. Rennes, 28 avril 2015.

Cass. Crim., 20 mai 2015, pourvoi n°14-81336, Bull. Crim. 2015, n°119.

Cass. Crim., 8 septembre 2015, n°15-85587, Bull. Crim. 2015, n°191.

Cass. Civ., 3 novembre 2016, n°1184, ECLI:FR:CCASS:2016:C101184.

6) Délibérations de la CNIL

Commission Nationale de l'Informatique et des Libertés, Délibération n°81-120 du 15 décembre 1981 *portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile*, JORF du 15 décembre 1981, n°34, p. 1210.

Commission Nationale de l'Informatique et des Libertés, Délibération n°85-73 du 9 juin 1981 *portant modification de la délibération n°81-77 du 9 juin 1981 concernant une recommandation relative à la collecte et au traitement d'informations nominatives relatives à des opinions politiques, philosophiques ou religieuse ou faisant apparaitre les origines raciales ou les appartenances syndicales par les entreprises privées de sondage*, JORF du 28 janvier 1986, p. 1543.

Commission Nationale de l'Informatique et des Libertés, Délibération n°00-015 du 21 mars 2000 *portant avis sur le traitement automatisé d'informations nominatives, mis en œuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales*, Publiée sur Légifrance le 14 octobre 2015.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2005-110 du 26 mai *2005 relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle*, Publiée sur Légifrance le 14 octobre 2014.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2005-237 du 18 octobre 2005 *portant refus d'autorisation de la mise en œuvre par la Société civile des Producteurs de Phonogrammes en France (PPF) d'un traitement de données à caractère personnel, ayant pour finalités, d'une part, la constatation des délits de contrefaçons commis via les réseaux d'échanges de fichiers dénommés « peer to peer », d'autre part, l'envoi de messages pédagogiques informant les internautes sur les sanctions prévues en matière de délit de contrefaçons*, Publiée sur Légifrance le 14 octobre 2014.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2010-336 du 22 juillet 2010 *autorisant la mise en œuvre par la société Morpho d'un traitement de données à caractère personnel ayant pour finalité principale la recherche sur les algorithmes biométriques,* Publiée sur Légifrance le 14 octobre 2015.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2011-035 du 17 mars 2011 *prononçant une sanction pécuniaire à l'encontre de la société X*, Publiée sur Légifrance le 13 décembre 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2011-193 du 28 juin 2011 *prononçant une sanction pécuniaire de 10 000€ à l'encontre de la société X*, Publiée sur Légifrance le 13 décembre 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2012-209 du 21 juin 2012 *portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (norme simplifiées n°48),* JORF du 13 juillet 2012, texte n°72.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., Publiée sur Légifrance le 10 janvier 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2015-078 du 5 mars *2015 portant avis sur un projet de loi relative au renseignement*, Publiée sur Légifrance le 25 mars 2015.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2015-155 du 1 juin 2015 *prononçant une sanction pécuniaire à l'encontre de la société X*. Publication non datée.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2015-454 du 21 décembre 2015 *prononçant un avertissement public à l'encontre de la société Profils Seniors*, Publiée sur Légifrance le 15 janvier 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-007 du 26 janvier 2016 *mettant en demeure les sociétés Fracebooks Inc. et Facebook Ireland*, Publiée sur Légifrance le 10 février 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération de la formation restreinte n°2016-053 du 1 mars 2016 *prononçant un avertissement à l'encontre de la société NC Numéricâble*, Publiée sur Légifrance le 9 mars 2016.

Commission Nationale de l'Informatique et des Liberté, Délibération n°2016-054 du 10 mars 2016 de la formation restreinte *prononçant une sanction pécuniaire à l'encontre de la société Google Inc.,* Publiée sur Légifrance le 26 mars 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-186 du 30 juin 2016 *portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maitrise par la personne concernée sur son gabarit biométrique*, AU-052, JORF n°0225 du 27 septembre 2016, texte n°53

Commission Nationale de l'Informatique et des Libertés, Délibération n°2016-187 du 30 juin 2016 *portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable de traitement*, AU-053, JORF n°0225 du 27 septembre 2016, texte n°52

Commission Nationale de l'Informatique et des Libertés, délibération de la formation restreinte n°2016-406 du 15 décembre 2016 *prononçant une sanction pécuniaire à l'encontre de la société Meetic SAS*, Publiée sur Légifrance le 30 décembre 2016.

Commission Nationale de l'Informatique et des Libertés, Délibération n°2017-013 du 19 janvier 2017 *autorisant l'Assistance Publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité un entrepôt de données de santé, dénommé EDS*, Publiée sur Légifrance le 4 mars 2017.

2 – Textes et décisions d'origine Européenne

1) Règlements

Règlement (CE) nº 515/97 du Conseil du 13 mars 1997, *relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole*, Journal Officiel de l'Union Européenne du 22 mars 1997, L 082, p. 0001 – 0016.

Règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000, *concernant la création du système «Eurodac» pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin*, Journal Officiel de l'Union Européenne du 15 décembre 2000, L 316, p. 1.

Règlement (CE) n°460/2004 du Parlement Européen et du Conseil du 10 mars 2004, *Instituant l'Agence Européenne chargée de la sécurité des réseaux et de l'information*, Journal Officiel de l'Union Européenne du 13 mars 2004. L 77.

Règlement (CE) n°2252/2004 du Conseil, du 13 décembre 2004 *établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres*, Journal officiel de l'Union Européenne du 29 décembre 2004, L 385/1.

Règlement (CE) n°1007/2008 du Parlement Européen et du Conseil du 24 septembre 2008, *modifiant le règlement CE n°460/2004 Instituant l'Agence Européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée*, Journal Officiel de l'Union Européenne du 13 mars 2004, L 293, pp. 1-2.

Règlement (CE) n°428/109/CE du Conseil du 5 mars 2009, *instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage*, Journal officiel de l'Union Européenne du 29 mars 2009, OJ L 134, pp. 1-269.

Règlement (CE) n°580/2011 du Parlement Européen et du Conseil du 8 juin 2011, *modifiant le règlement CE n°460/2004 Instituant l'Agence Européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée*, Journal Officiel de l'Union Européenne du 24 juin 2011, pp. 3-4.

Règlement (UE) n °1024/2012 du Parlement européen et du Conseil du 25 octobre 2012, *concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur et abrogeant la décision 2008/49/CE de la Commission («règlement IMI»),* Journal Officiel de l'Union Européenne du 14 novembre 2012, L 316, p. 1.

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*, 4 mai 2016, Journal officiel de l'Union Européenne du 4 mai 2016, L 119/1.

2) Directives

Directive 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995*, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Journal Officiel de l'Union Européenne n°L281, 23 novembre 1995, pp. 0031-0050.

Directive 1999/93/CE du Parlement Européen et du Conseil, du 13 décembre 1999, *sur un cadre communautaire pour les signatures électroniques*, Journal Officiel de l'Union Européenne n° L013, 19 janvier 2000, pp. 00012-0020.

Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000, *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (Directive sur le commerce électronique),* Journal Officiel de l'Union Européenne n°L178 du 17 juillet 2000, pp. 0001-0016.

Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002*, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)*, Journal Officiel de l'Union Européenne n°L201, 31 juillet 2002, pp. 37-47.

Directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009, *modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal Officiel de l'Union Européenne n°L337/11, 18 décembre 2009.

Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011, *relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil*, Journal Officiel de l'Union Européenne n°L304, 22 novembre 2011, po. 64–88.

Directive 2014/107/UE du Conseil du 9 décembre 2014, *modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal*, Journal Officiel de l'Union Européenne n°L359, 16 décembre 2014, pp. 1-29.

Directive 2016/680 du Parlement Européen et du Conseil du 27 avril 2016, *relative à la protection des personnes physiques à l'égard du traitement de 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/JAII du Conseil*, Journal Officiel de l'Union Européenne n°L119/89, 4 mai 2016.

Directive 2016/681 du Parlement Européen et du Conseil du 27 avril 2016, *relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière*, Journal Officiel de l'Union Européenne n°L119, 4 mai 2016, pp. 132-149.

3) Conventions

Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales telle qu'amendée par les Protocoles n°11 et n°14, Rome, 4 novembre 1950.

Convention Européenne d'entraide judiciaire en matière pénale, STE n° 30, signée à Strasbourg le 20 avril 1959.

Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981.

Charte des Droits Fondamentaux de l'Union Européenne, 2000/C 364/01, Journal Officiel des Communautés Européennes, 18 décembre 2000.

Convention n° 180 sur l'information et la coopération juridique concernant les "Services de la Société de l'Information", Moscou, 4 octobre 2001.

Deuxième protocole additionnel à la convention Européenne d'entraide judiciaire en matière pénale, STE n° 182, signé à Strasbourg le 8 novembre 2001.

Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données, STE n° 181, signé le 8 novembre 2001, en vigueur depuis le 1er juillet 2004.

Convention du Conseil de l'Europe sur la cybercriminalité faite à Budapest le 23 novembre 2001.

Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme, STCE n° 198, signée à Varsovie le 16 mai 2005.

Protocole d'amendement à la Convention concernant l'assistance administrative mutuelle en matière fiscale, STCE n° 208, signé à Paris le 27 mai 2010.

4) Décisions de la CEDH

CEDH, 30 mai 1974, *X. c. Belgique*, n°5488-72.

CEDH, 7 décembre 1976, *Handyside c. Royaume-Uni*, n°5493/72.

CEDH, 12 juillet 1977, *Brüggeman et Scheuten c. RFA*, n° 6959/75.

CEDH, 22 octobre 1981, *Dudgeon c. Royaume Uni*, n°3198034/51.

CEDH, 11 janvier 1991, *Buckley c. Royaume-Uni*, n°20348/92.

CEDH, 25 mars 1992, *Botella c. France*, n°57/1990/248/319.

CEDH, 16 décembre 1992, *Niemietz c. Allemagne*, n°13710/88.

CEDH, 25 mars 1993, *Costello-Roberts c. Royaume-Uni*, n°13134/87.

CEDH, 22 avril 1993, *Modinos c. Chypre*, n°7/1992/352/426.

CEDH, 22 février 1995, *Van Den Dungen c. Pays-Bas*, n°22838/93.

CEDH, 24 février 1998, *Botta c/Italie*, n°21439/93.

CEDH, 27 septembre 1999, *Smith et Grady c. Royaume-Uni*, n°33985/96 et n°33986/96.

CEDH, 21 décembre 1999, *Salgueiro da Silva Mouta c. Portugal*, n°33290/96.

CEDH, gr. ch., 16 février 2000, *Amann c. Suisse*, n° 27798/95.

CEDH, gr. ch., 11 juillet 2002, *Christine Goodwin c. Royaume-Uni*, n°28957/95.

CEDH, 29 juillet 2002, *Pretty c. Royaume Uni*, n° 2346/02.

CEDH, 9 janvier 2003, *L et V c. Autriche*, n°39392/92.

CEDH, 24 juillet 2003, *Karner c. Autriche*, n°40016/98.

CEDH, 4 décembre 2003, *M.C. c. Bulgarie*, n°39272/98.

CEDH, 24 juin 2004, *Von Hannover c. Allemagne*, n°59320/00.

CEDH, 17 février 2005, *K. A. et A. D. c. Belgique*, n° 42758/98 et 45558/99.

CEDH, 13 avril 2006, *Koteski c. République Yougoslave de Macédoine*, n°39630/09.

CEDH, 24 juillet 2008, *André et autres c. France*, n°18603/03.

CEDH, 2 décembre 2008, *KU c. Finlande*, n°2872/02.

CEDH, gr. ch., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, n° 30562/04 et 30566/04,

CEDH, 21 janvier 2010, *Xavier Da Silveira c. France*, n°43757/05.

CEDH, gr. ch., 7 février 2012, *Axel Springer Ag c. Allemagne*, n°39954/08

CEDH, 1er juillet 2014, *S.A.S. c. France*, n°43835/11.

CEDH, 18 novembre 2014, *Prokopovich c. Russie*, n°58255/00.

CEDH, 18 juillet 2016, *Keegan c. Royaume Uni*, n°28867/03.

CEDH, 22 juin 2017, *Aycaguer c. France*, n°8806/12.

CEDH, 11 juillet 2017, *Belcacemi et Oussar c. Belgique*, n°37798/13.

5) Décisions des juridictions de l'UE

CJCE, 20 mai 2003, *Österreichischer Rundfunk et a., aff. jtes*. C-465/00, C-138/01 et C-139/01.

CJCE, 6 novembre 2003, *Bodil Lindqvist*, aff. C-101/01.

CJCE, gr. ch., 5 octobre 2004, *X. c. Deutsches Rotes Kreuz*, aff . C-397/01 à C-403/01.

CJUE gr. ch., 23 mars 2010, *Google Inc. V. Louis Vuitton Malletier Sa*., aff. C-236/08.

CJUE gr. ch., 5 mai 2011, *Deutsche Telekom AG c/ Bundesrepublik Deutschland*, aff. C-543/09.

CJUE, 11 décembre 2011, *Frantisek Rynes c. Urad pro ochranu osobnich udaju*, aff. C-212/13.

CJUE, gr. ch., 13 mai 2014, *Google Span SL, Google Inc. c. Agencia Espanola de la Proteccion de Datos et Mario Costeja Gonzalez*, aff. C-131/12.

CJUE, gr. ch., 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14.

CJUE, 19 octobre 2016, *Breyer c. Bundesrepublik Deutschland*, aff. C-582/14.

CJUE gr. ch., 21 décembre 2016, *Tele2 Sverige AB c. Post-och Telestyrelsen*, aff. jtes. C-203/15 et C-698/15.

3 – Textes et décisions d'origine Internationale

1) Textes internationaux

Pacte international relatif aux droits civils et politique, Adopté et ouvert à la signature, à la ratification et à l'adhésion par l'Assemblée générale des Nations Unis dans sa résolution 2200 A (XXI) du 16 décembre 1966.

Déclaration Universelle des Droits de l'Homme, texte adopté le 10 décembre 1948 par l'assemblée générale des Nations Unies.

2) Textes et Décisions issues des juridictions étrangères

- *Afrique du Sud :*
  - Constitutional Court of South Africa, NM and Others v. Smith and Others (Freedom of Expression Institute as Amicus Curia), 2007, 5, SA 250 (CC), Case CCT 69/05

- *Allemagne :*
  - Datenschutz, Landesdatenschutezgesetz Vom 07/10/1970, Hessen
  - Bundes VerfassungsGericht. Volkszahlungsurteil, BVEerfGE Bd. 65, S. 1 FF, 15 Décembre 1983.
  - Bundesverfassungsgericht, 27 février 2008, aff. 1 BvR 370/07 et BVR 595/07.
  - Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 23. Dezember 2014 (BGBl. I S. 2438) geändert worden ist
  - LG Düsseldorf, Urteil vom 09/03/2016, Az.: 12 O 151/15.
  - Stellungnahme des Bundesrates, Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes, Deutscher Bundesrat: Drucksachen und Protokolle [BR-Drs.] 430/16 (Beschluss), Sept. 23, 2016.

- *Canada :*
  - Jugement de la Cour Suprême, 31 octobre 1997, Goodbout c. Longueuil (Ville), 1997, R.C.S, 844.
  - Supreme court of Canada, 28 juin 2017, Google Inc v. Equuustek Solution Inc, 2017 SCC 34.

- Etats-Unis :
  - Privacy Act of 1974, 5, U.S.C.
  - Lane v. Facebook, Inc, 709 F.3d791, 9 Circ.2013, 20 September 2012.
  - USA Freedom Act of 2015, H.R.2048, Public Law n°114-23, 6 February 2015.
  - *United States District Court for the Central District of California. Order compelling Apple Inc. to assist Agents in Search,* Retrieved February 27, 2016.

- *Campbell et al v. Facebook Inc*, Filing 202, Answer to Second Amended Complaint by Facebook Inc, Jessen, Joshua, Filed on 6/28/2016, Modified on 6/26/2016, VlkS, Court Staff.

- Suède:
  - DATALAG, Svensk Forfattningssamling [SFS] 1973 :289.

- Suisse:
  - Votation n°607 sur la loi fédérale du 25 septembre 2015 sur le renseignement, LRens.

- Royaume-Uni:
  - Investigatory Powers Act 2016, published by the Home Office the 1st March 2016.

VI - Sites Internet

Facebook.com

- Développeurs, Tokens d'accès, disponible sur https://developers.facebook.com/docs/facebook-login/access-tokens/ (consulté le 01/09/17).

- Facebook Business Help, disponible sur https://www.facebook.com/business/news/drive-and-measure-store-visits-and-sales (consulté le 01/09/17).

- Outil de gestion de création de campagne publicitaire, disponible sur https://www.facebook.com/ads/manager/creation/ (consulté le 01/09/2017).

- Pages d'aide, Comment puis-je supprimer une identification d'une photo ou d'une publication dans laquelle je suis identifié(e), disponible sur https://www.facebook.com/help/ (consulté le 01/09/2017).

- Politique d'utilisation des données, disponible sur https://fr-fr.facebook.com/about/privacy (consulté le 01/09/17).

- Règlement de la plateforme, disponible sur https://developers.facebook.com/policy/#control (consulté le 01/09/17).

- Social Plugins FAQs, General Questions, What information does Facebook get when I implement a social plugin, and how is it used, disponible sur https://developers.facebook.com/docs/plugins/faqs/ (consulté le 01/09/2017)

Google.com

- Règles de confidentialité de Google, disponible sur https://www.google.fr/intl/fr/policies/privacy/, (consulté le 01/09/2017)
- Google Adwords Help, About store visit conversions, disponible sur https://support.google.com/adwords/answer/6100636?hl=en (Consulté le 01/09/17).

Microsoft.com

- Utiliser la protection contre le tracking dans internet explorer, site internet de Microsoft, site internet de Microsoft, disponible sur http://windows.microsoft.com/fr-fr/internet-explorer/use-tracking-protection#ie=ie-11 , (consulté le 21/03/2016).

Safe Harbour

- Liste des entreprises associées, disponible sur https://safeharbor.export.gov/companyinfo.aspx?id=32284 (Consulté le 01/09/17).

Wikileaks

- Vault 7 Project, site internet de Wikileaks, disponible sur https://wikileaks.org/vault7/ (consulté le 01/09/17).

World Wide Web Consortium

- Site du W3C, Tracking protection working Group, disponible sur https://www.w3.org/2011/tracking-protection/. (consulté le 01/09/17).

VII - Normes Techniques

ISO/IEC 13335-1:2004, Technologies de l'information, Techniques de Sécurité, Gestion de la sécurité des technologies de l'information et des communications, norme annulée par la norme ISO/IEC 27000.

ISO/IEC 15408-1:2009, Technologies de l'information, Techniques de Sécurité, Critères d'évaluation pour la sécurité T1, publiée en décembre 2009.

ISO/IEC 270001 :2013, Technologies de l'information, Techniques de Sécurité, Systèmes de management de la sécurité de l'information, Exigence, publiée en octobre 2013.

ISO/IEC 270002 :2013, Technologies de l'information, Techniques de Sécurité, Code de bonne pratique pour le management de la sécurité de l'information, publiée en Octobre 2010.

ISO/IEC 270018 :2014, Technologies de l'information, Techniques de Sécurité, Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII, publiée en août 2014.

World Wide Web Consortium, *Device API Privacy Requirement*, W3C Working Group, 29 June 2010.

World Wide Web Consortium, *W3C Recommendations on HTML 5.1*, W3C Working Group, 1 November 2016.

Index

A Paragraphes

Autodétermination informationnelle 99, 136, 374

Autonomie décisionnelle 63, 102

Autorité administrative indépendante 185

B

Big Data 27, 207

C

Commission Nationale de l'Informatique et des libertés 13, 156

Consentement 13, 25, 315, 328

Consentement dématérialisé 525

Convention 108 477

Cookies 345

D

Dignité 89, 112

Directive 2002/58/CE 23

Directive 2016/681 29

Directive 95/46/CE 23

Donnée personnelle 13, 138, 299

Données sensibles 13, 199, 384

Droit à l'information 173

Droit à l'oubli 178

Droit à la protection des données 136

Droit au respect de la vie privée 48, 67, 91, 94, 150

Droit de rectification 176

Droit des données à caractère personnel 99, 133

Droits fondamentaux 5, 534

E

Echange de données 445

F

Fichier 151

G

Groupe de travail article 29 139

I

Informatique 135

Interface de Programmation Applicatives 454

Intimité de la vie privée 11, 104

L

Liberté d’expression 126

Liberté de disposer de son corps 114

Liberté de penser 79

Liberté personnelle 83

Llibertés individuelles 84

Loi du 7 octobre 2016 pour une République numérique 23

Loi Godfrain 245

Loi informatique et libertés 13

M

Manifestation de volonté 322, 499

N

National Security Agency 31, 214

P

Privacy by Design 274

Privacy by Default 304

Privacy Impact Assessment 280

Publicité comportementale 571

Q

Quadrature du net 24

R

Règlement général sur la protection des données 13

Relation asymétrique 507

S

Safe Harbour 447

Smart cities 27

Snowden 30, 214

T

Transparence 33, 153

V

Vie privée 48, 67, 91, 94, 150

Table des matières

Remerciements 1
Sommaire 2
Liste des principales abréviations 3

INTRODUCTION 6

Objet de l'étude 15
Contexte de l'étude 16
Périmètre de l'étude 26
Problématique de l'étude et annonce de plan 30

PARTIE I

L'ADAPTATION DU DROIT AU RESPECT DE LA VIE PRIVÉE À UN PHÉNOMÈNE TECHNOLOGIQUE.....32

TITRE I
L'ENCADREMENT JURIDIQUE D'UNE NOUVELLE FORME D'ATTEINTE A LA VIE PRIVEE 35

Chapitre I
La protection offerte par le droit au respect de la vie privée 37

Section 1
La protection de la faculté d'autonomisation 42
1 – L'identification des structures affectant la capacité décisionnelle 46
2 – Une protection de la liberté personnelle 50
3 – Un sanctuaire de la capacité décisionnelle des personnes 52
Conclusion 54

Section 2
La protection du périmètre objectif de la vie privée 58
1 – La protection du périmètre décisionnel physique 62
a) Le corps humain 62
b) Le domicile 66
2 – La protection du périmètre décisionnel informationnel 69
Conclusion 72

Chapitre 2
La protection offerte par le régime applicable aux données à caractère personnel 74

Section 1
Le régime applicable aux données à caractère personnel 77
1 – Les conditions relatives aux modalités du traitement 83
a) La loyauté et la licéité de la collecte 84
b) Finalité déterminée, explicite et légitime du traitement 86
c) Proportionnalité de la mise en œuvre 88
d) Caractère exact et complet des données 91
e) La durée de conservation 92

2 – Les droits conférés à la personne concernée 94
a) Droit d'information et d'accès 94
b) Droit de rectification, d'opposition, et d'effacement 96
c) Droit à la portabilité des données 99
d) Limitations 100
Conclusion 101

Section 2
La réduction conceptuelle du droit au respect de la vie privée dans l'innovation technologique 103
1 – L'absence de protection de la faculté d'autonomisation 104
2 – Le risque de patrimonialisation du régime protecteur des données à caractère personnel 108
Conclusion 110

TITRE II
L'APPLICABILITE DU DROIT DANS UN CONTEXTE TECHNOLOGIQUE MOUVANT 111

Chapitre 1
Le régime applicable aux nouvelles possibilités d'atteinte à la vie privée 116

Section 1
L'encadrement relatif des procédures d'acquisition de données par les services régaliens 118
1 – Le périmètre de collecte des interceptions judiciaires 121
2 – Le périmètre de collecte des interceptions administratives 126
Conclusion 129

Section 2
Les insuffisances du régime applicable aux atteintes aux systèmes de traitement de données 131
1 – La répression des atteintes aux systèmes de traitement de données 133
2 – La démocratisation des technologies d'anonymisation et de sécurisation des données 138
Conclusion 142

Chapitre 2
Une réinterprétation technique de la protection offerte par le régime 144

Section 1
L'intégration juridique de la Privacy by Design au processus d'innovation 146
1 – L'intégration technique de la Privacy By Design au processus d'innovation 149
2 – L'exemple de l'intégration potentielle d'une base de données à lien faible pour les passeports biométriques 151

Section 2
Les dangers d'une réinterprétation technique des mesures de protection 156
1 – Les conséquences d'une différence d'appréciation des standards de protection 158
2 – Le risque de dépossession normative porté par la PbD 161
Conclusion 163

Conclusion Partie I 164

PARTIE II

L'ADAPTATION DES ACTEURS DE L'INNOVATION AU RÉGIME PROTECTEUR DES DONNÉES À CARACTÈRE PERSONNEL 166

TITRE I
UNE PROTECTION LIEE AU CONSENTEMENT DE LA PERSONNE 171

Chapitre I
La place centrale du consentement dans la collecte des données 174

Section 1
La mise en place généralisée des conditions d'utilisation des services 175
1 – Une obligation juridique incontournable 177
2 – Une exception technique : les cookies de mesure d'audience 181
3 – La manifestation technique du refus de suivi de l'internaute 183
4 – Une nécessité économique 187
5 – vers un renforcement de la valeur du consentement lié aux règles de confidentialité 189
Conclusion 191

Section 2
Une collecte étendue légitimée par le consentement initial 193
1 – Une interprétation opportuniste des conditions de licéité du consentement dans la collecte des données 194
2 – La possibilité d'une collecte maximale des données par le recours systématique au consentement 198
3 – Une collecte des données possible grâce à l'accès au terminal de l'utilisateur 202
4 – Une acquisition des données étendue au dehors du périmètre dédié au service 205
5 – Une acquisition des données par interconnexion 209
Conclusion 212

Chapitre 2
La place centrale du consentement dans la valorisation des données 213

Section 1
Une innovation technique dépendante de la valorisation des données 214
1 – Exemple d'un large traitement de données : Google 215
2 – Un croisement des données fournies par les utilisateurs sur les utilisateurs : l'exemple de Facebook 217
3 – Une valorisation transnationale des données 220
Conclusion 223

Section 2
Une valorisation portée par les nouvelles capacités des APIs 224
1 – Les APIs : nouveaux outils d'interaction des bases de données 225
2 – Les APIs : moyens de contrôle et d'acquisition de l'information 227
3 – Le régime applicable aux APIs 228
4 – La répartition de la responsabilité dans l'exploitation d'une API 232
5 – Les règles techniques applicables à la conception d'une API 234
Conclusion 238

TITRE II
UNE PROTECTION ERODEE PAR LE RECOURS AU CONSENTEMENT 242

Chapitre 1
La remise en cause de la validité du consentement dans une relation asymétrique 247

Section 1
Les éléments fondateurs de la licéité du consentement 249
1 – La reconnaissance juridique du consentement dématérialisé 253
2 – Les conditions générales de licéités du consentement 257
3 – Les conditions spécifiques de licéités du consentement 261
a) « Toute manifestation de volonté » 261
b) «[…] Informée… » 265
c) « Spécifique » 267
d) « libre » 270
4 – Les notions connexes de la licéité du consentement 272
Conclusion 274

Section 2
La valeur du consentement dans la valorisation des données à caractère personnel 275
1 – Une manifestation de la volonté opportuniste 276
2 – Une obligation d'information à la portée relative 280
a) La compréhension de l'impact du traitement : le problème de l'asymétrie informationnelle 280
b) La compréhension de l'impact du traitement : le problème cognitif 283
3 – Une liberté de consentir illusoire 286
Conclusion 288

Chapitre 2
Les conséquences d'une remise en cause de la valeur du consentement 291

Section 1
La fragilité économique de l'innovation numérique 293
1 – La capacité de sanction financière de la CNIL 296
2 - La sanction d'incessibilité des fichiers illicites 298
Conclusion 300

Section 2
Pour une refonte des mécanismes de protection de la vie privée dans le cadre de l'innovation 302
1 – Les propositions de modifications des critères de validité du consentement 304
2 – Pour une refonte des mécanismes de protection de la vie privée dans l'innovation technologique 308
Conclusion 311

Conclusion Partie II 312

CONCLUSION GÉNÉRALE 313

BIBLIOGRAPHIE 317
I - Ouvrages 318
II - Articles 322
1 - Articles Scientifiques 322

2 - Articles de Vulgarisation Scientifique 326
3 - Articles d'Actualité 328
III - Thèses et Rapports Spécialisés 331
1 - Thèses 331
2 - Rapports 331
IV – Communications, Avis et Déclarations Publiques 334
1 – Communications de l'ANSSI 334
2 - Communications de la Commission Européenne 334
3 – Communications de la CNIL 336
4 - Communications et Avis du G29 et du Contrôleur Européen 338
5 – Autres Communications 340
V - Références Normatives 342
1 – Textes et décisions d'origine nationale 342
2 – Textes et décisions d'origine Européenne 351
3 – Textes et décisions d'origine Internationale 356
VI - Sites Internet 358
VII - Normes Techniques 360

INDEX 361
TABLE DES MATIERES 364
ANNEXE 369

Annexe

Privacy and Data Protection Impact Assessment Framework for RFID Applications

12 January 2011

INDEX

1. Introduction..... 3
1.1. Key Concepts..... 4
1.2. Internal Procedures 5

2. The PIA Process..... 6
2.1. Initial Analysis Phase..... 7
2.2. Risk Assessment Phase..... 8

3. Final Provision..... 11

ANNEX I - Characterisation of the RFID Application Description..... 12

ANNEX II - Privacy Targets..... 13

ANNEX III - Privacy Risks..... 14

ANNEX IV - Examples of RFID Application Controls and Mitigating Measures..... 17

Appendix A: References..... 21

Appendix B: Glossary..... 23

. Introduction

The European Commission ("the Commission") issued a Recommendation dated 12 May 2009 on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification ("RFID Recommendation"). In that Recommendation, the Commission established a requirement for the endorsement by the Article 29 Data Protection Working Party of an industry-prepared framework for Personal Data and Privacy impact assessments of RFID Applications. These assessments are commonly referred to as privacy impact assessments, or PIAs. This RFID Application PIA Framework ("the Framework") addresses that requirement.

The benefits of conducting PIAs for RFID Applications are numerous. These include helping the RFID Application Operator:

- to establish and maintain compliance with privacy and data protection laws and regulations;
- to manage risks to its organisation and to users of the RFID Application (both privacy and data protection compliance-related and from the standpoint of public perception and consumer confidence); and
- to provide public benefits of RFID Applications while evaluating the success of privacy by design efforts at the early stages of the specification or development process.

The PIA process is based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices.

The PIA process is designed to help RFID Application Operators uncover the privacy risks associated with an RFID Application, assess their likelihood, and document the steps taken to address those risks. These impacts (if any) could vary significantly, depending on the presence or lack of personal information processing by the RFID Application. The PIA Framework provides guidance to RFID Application Operators on the risk assessment methods, including adequate measures to mitigate any likely data protection or privacy impact in an efficient, effective and proportionate manner.

Finally, the PIA Framework is sufficiently general to be applicable to all RFID Applications, while allowing for particularities and specificities to be addressed at Sectoral or Application type level.

The PIA Framework is part of the context of other information assurance, data management, and operational standards that provide good data governance tools for RFID and other Applications. The current Framework could be used as a basis for the development of industry-based, sector-based, and/or application-based PIA templates. As in the implementation of any theoretical document, the PIA Framework may require clarification of its application of terms, as well as guidance on practices that should be based on practical experience, that may help in its implementation.

1.1. Key Concepts

There are a number of key concepts used in the Framework that warrant description. ***RFID*** is a technology that uses electromagnetic waves to communicate with RFID Tags, with the possibility of reading the unique identification numbers of the RFID Tags or perhaps other information stored in them. ***RFID Tags*** are generally small and can take many forms, but are often composed of electronic memory that is readable and perhaps writable, and antennae. ***RFID Readers*** are used to read the information on RFID Tags.

RFID Applications process information developed through the interaction of RFID Tags and RFID Readers. Such Applications are operated by one or more ***RFID Application Operators*** and are supported by back-end systems and networked communication infrastructures. If an RFID Application Operator makes determinations related to the collection or use of personal data, its role could be similar to that of the Data Controller as defined in Directive 95/46/EC and would be described as the natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an RFID Application which has impacts or personal information.

In the context of RFID technology, the following taxonomy applies:

- A ***Privacy Impact Assessment (PIA)*** is a process whereby a conscious and systematic effort is made to assess the privacy and data protection impacts of a specific RFID Application with the view of taking appropriate actions to prevent or at least minimise those impacts.
- The ***Framework*** identifies the objectives of RFID Application PIAs, the components of RFID Applications to be considered during PIAs, and the common structure and content of RFID Application PIA Reports.
- A ***PIA Report*** is the document resulting from the PIA Process that is made available to competent authorities. Proprietary and security sensitive information may be removed from PIA Reports before the Reports are provided externally (e.g., to the competent authorities) as long as the information is not specifically pertinent to privacy and data protection implications. The manner in which the PIA should be made available (e.g., upon request or not) will be determined by member states. In particular, the use of special categories of data may be taken into account, as well as other factors such as the presence of a data protection officer.
- ***PIA Templates*** may be developed based on the Framework to provide industry-based, application-based, or other specific formats for PIAs and resulting PIA Reports.

These and other terms, such as ***Users*** **and** ***Individual***, are for the purpose of this PIA Framework also described in Appendix B: Glossary. Terms from Directive 95/46/EC related to data protection are incorporated by reference.

The execution and reporting, where appropriate, of PIAs are in addition to other obligations that the RFID Application Operators may have under specific applicable laws, regulations, and other binding agreements.

1.2. Internal Procedures

RFID Application Operators should have their own internal procedures to support the execution of PIAs, such as the following:

- *Scheduling of the PIA process* so that there is sufficient time to make any needed adjustments to the RFID Application and to make the PIA Report available to the competent authorities at least six weeks before deployment.
- *Internal review of the PIA process (including the initial analysis) and PIA Reports* for consistency with other documentation related to the RFID Application, such as system documentation, product documentation, and examples of product packaging and RFID Tag implementation. The internal review should provide a feedback loop to address any impacts collected after the Application is implemented and to accommodate results from prior PIAs.

- *Compilation of supporting artefacts* (that may include results of security reviews, controls designs and copies of notices) as evidence that the RFID Application Operator has fulfilled all of the applicable obligations.
- *Determination of the persons and/or functions within the organisation who have the authority for relevant actions* during the PIA process (e.g., completion of the PIA initial analysis and PIA Report, signing the PIA Report, maintaining applicable documents, and any separation of duties for these functions).
- *Provision of criteria for how to evaluate and document whether the Application is ready or not ready for deployment* consistent with the Framework and any relevant PIA Template.
- *Consideration/Identification of factors that would require a new or revised PIA Report* is warranted. Criteria should include: significant changes in the RFID Application, such as material changes that expand beyond the original purposes (e.g., secondary purposes); types of information processed; uses of the information that weaken the controls employed; unexpected personal data breach[1] with determinant impact and which wasn't part of the residual risks of the application identified by the first PIA; defining of a period of regular review; responding to substantive or significant internal or external stakeholder feedback or inquiry; or significant changes in technology with privacy and data protection implications for the RFID Application at stake. Material changes that would narrow the scope of collection or use would not trigger per se the need for a revised PIA. Throughout the lifetime of the RFID Application, a new or revised PIA Report would be warranted if the RFID Application changes in level as described in the Initial Analysis Section.
- *Stakeholder Consultation.* Opinions and feedback from relevant stakeholders related to the RFID Application under review should be appropriately considered as part of the PIA review of potential concerns and issues. Consultations should be appropriate to the scale, scope, nature, and level of the RFID Application. Within companies, individuals are designated with responsibility for overseeing and assuring organisational or departmental privacy. These individuals are essential participants in the PIA process to the extent that they are involved in the particular RFID Applications or their oversight. Employees with knowledge of technical, marketing and other disciplines may also be needed participants in the process, depending upon the nature of the RFID Application and their relation to it. RFID Operators may have consultation mechanisms by which external stakeholders, whether individuals, organisations or authorities, can interact with them and provide feedback. As far as is appropriate, the RFID Operator should use consultation mechanisms to gain input from the groups representing the individuals whose privacy will be directly impacted by the proposals, e.g. employees and customers of the RFID operator.

2. The PIA Process

The purpose of the Framework is to provide guidance to RFID Application Operators for conducting PIAs on specific RFID Applications, as called for in the Recommendation, and to define the common organisational structure and content categories of the PIA Reports in which the results from such PIAs have to be documented. In addition, because many RFID Application Operators within particular sectors may be considering the same or similar RFID Applications, the Framework provides a basis for the development of PIA Templates for particular Applications or industry sectors. PIA Templates can assist these sectors to conduct PIAs and produce the resulting PIA Reports for these similar RFID Applications

1 In this case the applicable definition shall be the one provided in the directive 2009/136/EC amending directive 2002/58 see page 29 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

more efficiently[2]. Because common RFID Applications may be offered in a number of Member States, the Framework is designed to harmonise requirements for RFID Application Operators consistent with local laws, regulations, best practices and other binding agreements.

The Framework addresses the process for conducting PIAs of RFID Applications before deployment and specifies the scope of resulting PIA Reports.[3]

RFID Application Operators must develop a PIA for each RFID Application they operate. If they deploy several related RFID Applications (potentially in the same context or at the same premises) they may create one PIA Report if the boundaries and differences of the Applications are explicitly described in the PIA Report. If RFID Application Operators reuse one RFID Application in the same way for multiple products, services or processes, they may create one PIA Report for all products, services or processes that are similar (for example, a car manufacturer deploying the same anti-theft mechanisms in all cars and under the same service conditions) . The execution and reporting, where appropriate, of PIAs are in addition to other obligations that the RFID Application Operators may have under specific applicable laws, regulations, and other binding agreements.

The PIA process has two phases:

1. **Initial Analysis Phase**: the RFID Application Operator will follow the steps outlined in this Section to determine:

   a) whether a PIA of its RFID Application is required or not; and

   b) if a Full or Small Scale PIA is warranted.

2. **Risk Assessment Phase**: it outlines the criteria and elements of Full and Small Scale PIAs.

2.1. Initial Analysis Phase

As a prerequisite to conducting a PIA for a specific Application, each organisation must understand how to implement such a process based on the nature and sensitivity of the data it deals with, the nature and type of processing or stewardship of information it engages in, and the type of RFID Application in question. For those organisations that may already have privacy risk assessment processes in place for other Applications, the classification criteria and process steps should help them map their existing PIA processes to this Framework.

To conduct the initial assessment, an RFID Application Operator has to go through the decision tree depicted in Figure 1. This will help the RFID Application Operator to determine whether and to what extent a PIA is needed for the RFID Application at hand.

The resulting level in the initial analysis phase helps determine the level of detail necessary in the risk assessment (e.g., either a Full Scale or Small Scale PIA).

This initial analysis must be documented and made available to data protection authorities upon request. For documentation guidelines, please see Annex I.

---

[2] The concept of mutual or multiple recognition across entities and sectors for the deployment of previously vetted RFID Applications should be explored.

[3] Point 5 (a) of the European Commission Recommendation of May 2009 on the implementation of privacy and data protection principles in Applications supported by radiofrequency identification C(2009) 3200 final.

Full Scale PIA

A Full Scale PIA is required for Applications that are determined to be Level 2 or Level 3 by the initial analysis phase in Section 2.1. Examples of Applications requiring a Full Scale PIA include Applications that process personal information (Level 2) or where the RFID Tag contains personal data (Level 3). While both Level 2 and Level 3 result in a Full Scale PIA, they identify different risk environments and as such will have different mitigation strategies. For example, Level 2 Applications may have controls to protect back-end data while Level 3 Applications may have controls to protect both back -end data and tag data. Industry may further refine these levels and how they impact the PIA process with further experience. Since the Application processes personal data, a highly detailed risk assessment (Full Scale) is necessary to ensure that mitigations are well elaborated. This will help the RFID Application Operator to identify relevant risks and develop appropriate controls. In this context, Operators should also consider whether the RFID Tag's information is likely to be used beyond the initial purpose or context understood by the individual, particularly if it could be used to process or link to personal data, and whether a new PIA analysis is warranted or other mitigating controls should be employed.

Small Scale PIA

Small Scale PIAs follow the same process as Full Scale PIAs, but given the lower risk profile a Small Scale PIA is more restricted in scope and level of detail in both the inquiry and the report than a Full Scale PIA. Small Scale PIAs are relevant for Level 1 Applications. While a Small Scale PIA follows a similar process to the Full Scale PIA, since the relevant risks of a Level 1 Application are lower than Level 2 or Level 3, the required controls and corresponding documentation in the PIA Report are simplified.

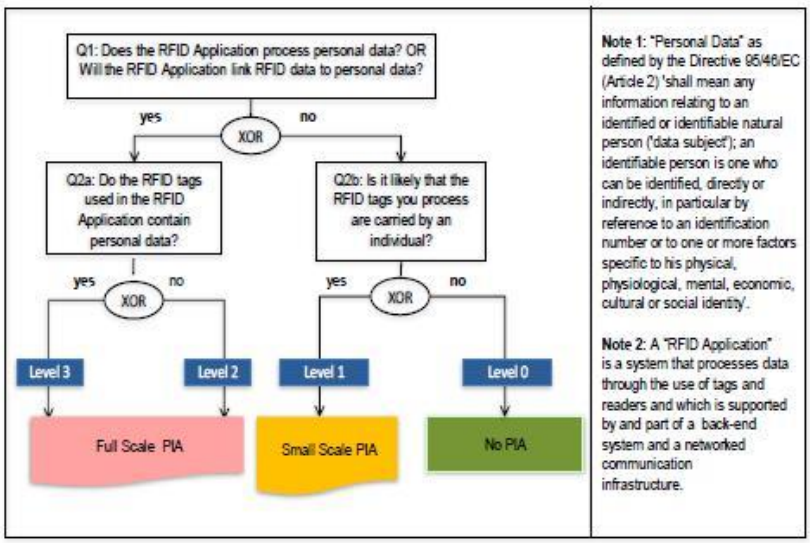


Figure 1: Decision Tree on whether and at what level of detail to conduct a PIA

2.2. Risk Assessment Phase

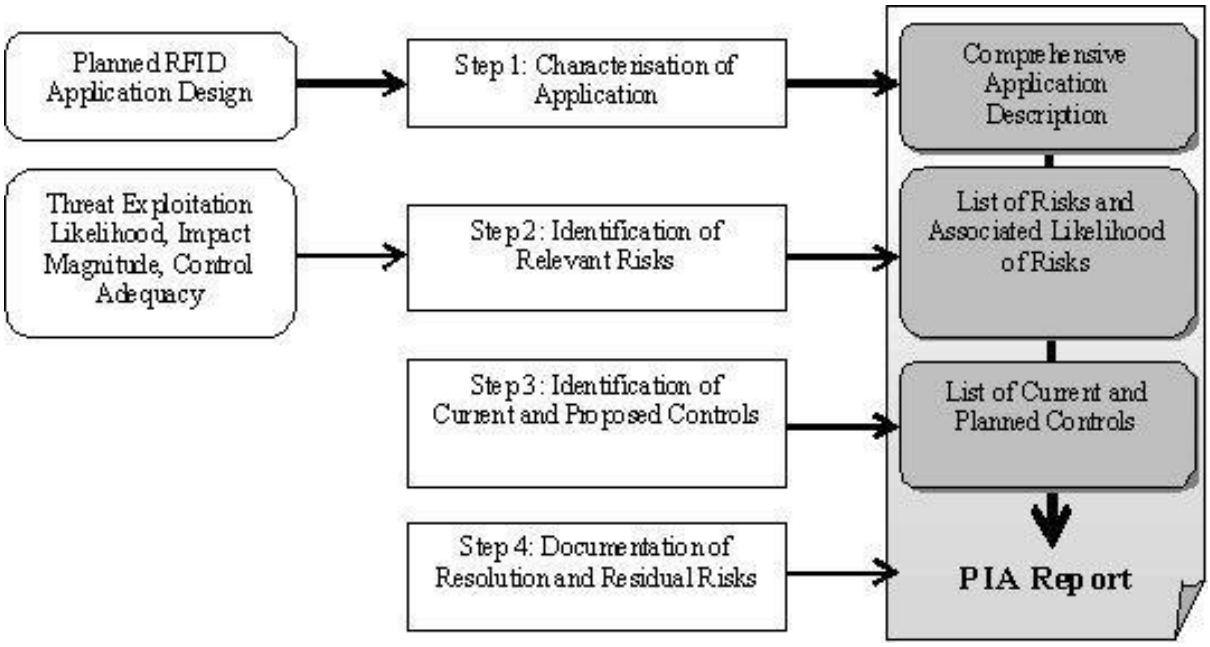
The objective of a risk assessment is to identify the privacy risks caused by an RFID Application - ideally at an early stage of system development - and to document how these risks are *pro- actively* mitigated through technical and organisational controls. In this way a PIA plays an important role in compliance and the legal requirements of privacy (Directive 95/46) and is a measure by which we judge the effectiveness of the mitigation procedures.

To save time and cost, it is recommended to run through this risk assessment phase well before final decisions on an RFID Application's architecture are taken so that technical privacy mitigation strategies can be embedded into the system's design, and do not need to be 'bolted on' later.

A risk assessment process typically considers in the first instance the risks of an RFID Application in terms of their likelihood of occurrence and magnitude of their consequences. RFID Application Operators are advised to use the privacy targets of the EU Directive as a starting point for their risk assessment (see Annex II). Privacy risks may be high, because the RFID Application implementation could be susceptible to malicious attacks or because organisational or environmental privacy controls do not exist. Privacy risks may also be small, simply because their occurrence is unlikely in the environment or organisation at hand, or because the RFID Application is already configured in a highly privacy friendly way. The PIA Process aims to consider all potential risks and then reflects on their magnitude, likelihood and potential mitigation. The result of this reflection is the identification of those privacy risks that are really relevant for the organisation's RFID deployment and that need to be mitigated through effective controls.

The PIA Process (as visualised in figure 2) requires any RFID Application Operator to:

1. Describe the RFID Application;
2. Identify and list how the RFID Application under review could threaten privacy and estimate the magnitude and likelihood of those risks;
3. Document current and proposed technical and organisational controls to mitigate identified risks; and
4. Document the resolution (results of the analysis) regarding the Application.



Step 1: Characterisation of Application

The Application characterisation should give a comprehensive and full picture of the Application, its environment and system boundaries. The Application design, its adjacent interfaces with other systems, and information flows are described. Data flow diagrams that show processing of primary and secondary data are recommended to visualise information flows. Data structures need to be documented, too, so that potential links can be analysed. Annex I summarises the elements that characterise an RFID Application for the purposes of conducting a PIA.

In addition, information related to the Application's operational and strategic environment is recommended. This may include the system's immediate and longer-term mission, stakeholders in information collection, functional requirements, all potential users and a description of the RFID Application's architecture and data flows (in particular, interfaces to external systems that may process personal data).

Step 2: Identification of Risks

The goal of this step is to identify conditions that may threaten or compromise personal data using the EU Directive as a guide for important hallmarks of privacy targets to protect. Risks may be related to the RFID Application components, its operations (collection, storage and processing infrastructure) and the data sharing and processing environment in which it is embedded.

A list of potential privacy risks may be found in Annex III. They serve as a guide for a systematic identification of potential risks that threaten the EU Directive targets (Annex II).

In addition to the identification of risks, a PIA requires a relative quantification of these risks. An RFID Application Operator should consider, as informed by the principles of proportionality and under reasonable terms, the *likelihood* of privacy risks occurring. Risks can occur from within, and where warranted, outside of the particular RFID Application at hand. These risks may be derived from both the likely uses and possible misuses of the information, and in particular if the RFID Tags used within the RFID Application remain operational once in possession of individuals**.**

The risk assessment requires evaluating the applicable risks from a privacy perspective; the RFID Operator should consider:

1. The significance of a risk and the likelihood of its occurrence.
2. The magnitude of the impact should the risk occur.

The resulting risk level can then be classified as low, medium or high.

A risk that has caused a prime subject of debate is that RFID Tags could be used for the profiling and/or tracking of individuals. In this case the RFID Tag's information – in particular its identifier(s) – would be used to re-identify a particular individual. Retailers who pass RFID Tags on to customers without automatically deactivating or removing them at the checkout *may* unintentionally enable this risk. A key question, though, is whether this risk is likely and actually materialises into an *undismissable* risk or not. According to point 11 of the RFID Recommendation, retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy in accordance with this Framework, give their consent to keep the tags operational.

Retailers are not required to deactivate or remove tags if the PIA report concludes that tags that are used in a retail application and would remain operational after the point of sale do

not represent a likely threat to privacy or the protection of personal data as stated in point 12 of the same Recommendation. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer.

Sector specific templates that shall be developed over time on the basis of this Framework and for use in different industries may inform risk identification in greater detail.

Step 3: Identification and Recommendation of Controls

The goal of this step is to analyse the controls that have been implemented or are planned for implementation, to minimise, mitigate or eliminate the identified privacy risks.

Controls are either of a technical or nontechnical nature. Technical controls are incorporated into the Application through architectural choices or technically enforceable policies, e.g. default settings, authentication mechanisms, and encryption methods. Nontechnical controls on the other hand are management and operational controls, e.g. operational procedures. Controls can be categorised as being preventive or detective. The former ones inhibit violation attempts and the latter ones warn of violations or attempted violations.

There can also be 'natural' controls created by the environment. For example, if there are no readers installed that could conduct a tracking of items or individuals (i.e. because there is no business case for it), then naturally there is also no (likely) risk.

The identified risks and their associated risk levels should guide the decision on which of the identified controls are relevant and thus need to be implemented. The PIA documentation should explain how the controls relate to specific risks, and should elaborate on how this mitigation will result in an acceptable level of risk.

Examples of controls are provided in Annex IV.

Step 4: Documentation of Resolution and Residual Risks

Once the risk assessment has been completed, the final resolution about the Application should be documented in the PIA Report, along with any further remarks concerning risks, controls and residual risks.

- An RFID Application is approved for operations once the PIA Process has been completed with relevant risks identified and appropriately mitigated to assure no significant residual risks remain in order to meet the requirements of compliance, with appropriate internal reviews and approvals.

- Where an RFID Application is not approved for operations in its current state, further consideration will require a specific corrective action plan to be developed, and a new privacy impact assessment to be completed in order to determine if the Application has reached an approvable state.

The resolution should be associated with the following information:

- Name of the person signing the resolution.
- Title of the person.
- Date of the resolution.

PIA Report

PIAs are internal processes containing sensitive information that can have security implications as well as potentially confidential and proprietary information of the company related to products and processes. That said, a PIA report should typically include:

1. The Description of the RFID Application as outlined in ANNEX I.

2. Documentation of the four steps outlined above.

The signed PIA Report that contains an approved resolution should be given to the assigned company's data privacy/security official in accordance with the RFID Application Operator's internal procedures. This report is provided without prejudice to the obligations set forth in the Directive 95/46/EC for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC.

3. Final Provision

The PIA Framework will take effect no later than 6 months after publication and endorsement by the Article 29 Data Protection Working Party. For RFID Applications in place before the PIA Framework takes effect, the PIA Framework will apply only when the conditions are met for documenting a new or revised PIA in accordance with the PIA Framework.

ANNEX I - *Characterisation of the RFID Application Description*

The RFID Application Operator should include, where applicable, the below information in the PIA Report.

RFID Application Operator	• Legal entity name and location • Person or office responsible for PIA timeliness • Point(s) of contact and inquiry method to reach the Operator
RFID Application Overview	• RFID Application name • Purpose(s) of RFID Application(s) • Basic use case scenarios of the RFID Application • RFID Application components and technology used (i.e. Frequencies, etc.) • Geographical scope of the RFID Application • Types of users/individuals impacted by the RFID Application • Individual access and control
PIA Report Number	• Version Number of PIA Report (distinguishing new PIA or just minor changes) • Date of last change made to PIA Report
RFID Data Processing	• List of types of data elements processed • Presence of Sensitive information in the data being processed, e.g., health
RFID Data Storage	• List of types of data elements stored • Storage duration
Internal RFID Data Transfer (if applicable)	• Description or diagrams of data flows of internal operations involving RFID data • Purpose(s) of transferring the personal data
External RFID Data Transfer (if applicable)	• Type of data recipient(s) • Purpose(s) for transfer or access in general • Identified and/or identifiable (level of) personal data involved in transfer • Transfers outside the European Economic Area (EEA)

ANNEX II - *Privacy Targets*

There are today 9 privacy targets embedded in the Directive 95/46/EC. The PIA Process was developed by considering these targets and the associated risks of RFID. This Annex summarises these privacy targets. While all targets are essential elements of organisational compliance, in many cases only a subset of these requirements will be at issue in the RFID Application under consideration. Thus the role of these targets is to inform the creation and development of the PIA process more than the operation of any specific PIA.

Description of privacy target (taken and updated from the respective EU Privacy Directive(s); here Directive 95/46/EC)	
Safeguarding quality of personal data	Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
Legitimacy of processing *sensitive* personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially.
Safeguarding confidentiality and security of processing	Preventing unauthorised access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
Compliance with data retention Requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements

ANNEX III - *Privacy Risks*

This section provides a list of possible privacy risks related to the use of the RFID Application under review. It is recommended that – in particular for Full Scale PIAs - risks are systematically identified with the help of standard risk assessment procedures that would include threats and vulnerabilities to an RFID Application.

The table below provides examples of risks that may affect an entity's ability to meet the privacy targets described in Annex II. RFID Application Operators can use this list as a starting point; however, not all of these risks may apply to all RFID Applications. RFID Operators should make sure each identified risk is appropriately mitigated by one or more controls in light of the likelihood of risk occurrence and magnitude of impact. RFID Application Operators may need to combine controls or augment existing controls based on factors including the technology in use, nature of their implementation, type of information, and applicable policies, among others.

Privacy Risk	**Description and example**
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. Example: No documentation of purposes for which RFID data is used and/or use of RFID data for all kinds of feasible analysis.
Collection exceeding purpose	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. Example: RFID payment card information is not only used for the purpose of processing transactions but also to build individual profiles.
Incomplete information or lack of transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. Example: RFID Information available to consumers that lacks clear information on how RFID data is processed and used, the identity of the Operator, or the user's rights.
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose. Example: RFID payment card information is combined with personal data obtained from a third party.
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose. Example: Personal data is collected as part of the Application and is saved for longer than

	legally allowed.
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage. Example: Cannot return/exchange/use legal warranties for products when RFID Tag is deactivated or removed.
Secret data collection by RFID Operator	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. Example: Consumer information is read while walking in front of stores or in mall and no Logo or Emblem is warning him or her about RFID readouts.
Inability to grant access	There is no way for the data subject to initiate a correction or erasure of his data. Example: Employer cannot give employee a full picture of what is saved about him or her on the basis of RFID access and manufacturing data.
Prevention of objections	There are no technical or operational means to allow complying with a data subject's objection. Example: Hospital visitor cannot opt out of reading out sensitive personal information on tags (i.e. medications).
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decision-making. Example: Without notice to consumers, an RFID Operator reads all tags carried by an individual, including tags provided by another entity, and determines what type of marketing message the individual should receive based on the tags.
Insufficient access right management	Access rights are not revoked when they are no longer necessary. Example: Through an RFID card, an ex-trainee gets access to parts of an enterprise where he or she should not.
Insufficient authentication mechanism	A suspicious number of attempts to identify and authenticate are not prevented. Example: Personal data contained on tags is not protected by default with a password or another authentication mechanism.
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation, etc. Example: An RFID Operator shares collected information with a third party without notice or

	consent as otherwise legally allowed.
Insufficient logging mechanism	The implemented logging mechanism is insufficient. It does not log administrative processes. Example: It is not logged who has accessed the RFID employee card data.
Uncontrollable data gathering from RFID Tags	The risk that RFID Tags could be used for regular profiling and/or tracking of individuals. Example: Retailer reads all tags that they can see.

ANNEX IV – *List of Examples of RFID Application Controls and Mitigating Measures*

This section provides a list of examples of potential controls that can help an RFID Application Operator to identify appropriate mitigating strategies. Risks identified as relevant for an RFID Application Operator in Step 2 of the PIA risk process can be mitigated through one or several mitigation strategies, some of which are outlined in this Annex IV. The goal is that by running through a PIA process, the RFID Application Operator identifies and implements the controls necessary to mitigate the relevant privacy risks.

Potential control mechanisms include:

- RFID Application Governing Practices.
- Individual access and control.
- System Protection Measures (including Security Controls).
- Tag Protection.
- Accountability Measures.

These practices are ancillary to the existing European Union data protection regulatory framework and are not intended to replace it or modify its scope.

RFID Application Governing Practices

Governing practices may include:

- Management practices by the RFID Application Operator.
- Disposal of and erasure policies for RFID data.
- Policies related to lawful processing of personal information.
- Provisions in place for data minimisation in handling RFID data, where feasible.
- Processing or storing of information from tags that do not belong to the RFID Operator.
- Security Governance practices.

Providing Individual Access and Control

- Providing information about the purposes of the processing and the categories of personal data involved.
- Description of how to object to the processing of personal data or withdraw consent.
- Identification of process to request rectification or erasure of incomplete or inaccurate personal data.

System Protection

System Protection with respect to the appropriate protection of privacy and personal data should also be documented in this Section of the PIA Report. System protection concepts apply to back-end systems and communication infrastructure in so far as they are relevant to the RFID Application. Where they do apply, it should be recognised that backend systems are often complex and may have been the subject of their own PIA. That analysis may need to be reviewed to assure that it considered information of the nature used by the RFID Application. Where no such PIA exists, the following components of the backend system should be considered:

- Access controls related to the type of personal data and functionality of the systems are in place.
- Controls and policies put in place to ensure the Operator does not link personal data in the RFID Application in a manner inconsistent with the PIA Report.
- Whether appropriate measures are in place to protect the confidentiality, integrity, and availability of the personal data in the systems and in the communication infrastructure.
- Policies on the retention and disposal of the personal data.
- Existence and implementation of information security controls, such as:
    - Measures that address the security of networks and transport of RFID data.
    - Measures that facilitate the availability of RFID data through appropriate back-ups and recovery.

RFID Tag Protection

RFID Tag Protection controls related to privacy and personal data should be indicated. They are particularly relevant to RFID Applications that use RFID Tags containing personal data.

These protection controls include the following:

- Access control to functionality and information, including authentication of readers, writers, and underlying processes, and authorisation to act upon the RFID Tag.
- Methods to assure/address the confidentiality of the information (e.g., through encryption of the full RFID Tag or of selective fields).
- Methods to assure/address the integrity of the information.
- Retention of the information after the initial collection (e.g., duration of retention, procedures for eliminating the data at the end of the retention period or for erasing the information in the RFID Tag, procedures for selective field retention or deletion).
- Tamper resistance of the RFID Tag itself.
- Deactivation or removal, if required or otherwise provided.

Mitigation can include user based controls that address situations where different needs or sensitivities related to privacy may be at issue. Deactivation or removal are currently the two most common forms of end-user/consumer mitigation. These may either be required as part of a PIA analysis, in certain circumstances by law or as a customer option after the point of sale to enhance confidence. In addition, the EC Recommendation on RFID Privacy and Data Protection for RFID Applications suggests certain methodologies and best practices associated with implementation of deactivation or removal in retail.[4]

Accountability Measures

These measures are designed to address procedural data protection, in the area of accountability. Through these measures external awareness regarding RFID Applications is raised.

- Ensuring the easy availability of a comprehensive **information policy** that includes:
  - Identity and address of the RFID Application Operator.
  - Purpose of the RFID Application
  - Types of data processed by the RFID Application, in particular if personal data are processed.
  - Whether the locations of RFID Tags will be monitored when possessed by an individual.
  - Likely privacy and data protection impacts, if any, relating to the use of RFID Tags in the RFID Application and the measures available to mitigate these impacts.
- Ensuring concise, accurate and easy to understand **notices** of the presence of RFID readers that include:
  - The identity of the RFID Application Operator.
  - A point of contact for Individuals to obtain the information policy.
- Noting if and how **redress mechanisms** are made available:
  - RFID Application Operator accountable legal entity (-ies) (may be one for each jurisdiction or operating area).
  - Point(s) of contact of the designated person or office responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures related to the protection of personal data and privacy.
  - Inquiry methods (e.g., methods through which the RFID Application Operator may be reached to ask a question, make a request, file a complaint, or exercise a right).

[4] Point 12/13 of the EC Recommendation of 12 May 2009. {SEC (2009) 585}: *Any deactivation or removal method should be made available free of charge, either immediately or at a later stage, without any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer.*

- Methods to object to processing, to exercise access rights to personal data (including deleting and correcting personal data), to revoke consent, or to change controls and other choices regarding the processing of personal data, if required or otherwise provided.

- Other redress methods, if required or otherwise provided.

Appendix A: References

This Section provides references to formal documents used to help develop the Framework.

- ☐ "Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio-frequency identification," Commission of the European Communities, 12 May 2009, C (2009) 3200, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

- ƒ "Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification," Summary of the Impact Assessment, Commission of the European Communities, 12 May 2009, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

- ☐ "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Communities, 23 November 1995, L 281/31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

- ☐ "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Official Journal of the European Communities, 31 July 2002, L 201/37, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

- ƒ "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," Official Journal of the European Union, 18 December 2009, *L* 337/11, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

- ƒ "Opinion 4/2007 on the concept of personal data," Article 29 Data Protection Working Party, 20 June 2007, 01248/07/EN WP 136, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

- ƒ "Privacy Impact Assessment Handbook," available at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

- "Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data," available at http://ec.europa.eu/ justice_home/fsj/privacy/law/implementation_en.htm

- "Working document on data protection issues related to RFID technology," Article 29 Data Protection Working Party, 19 January 2005, 10107/05/EN WP 105, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Appendix B: Glossary

A number of terms are used in the Framework related to the concepts of privacy and data protection, and to the Application of RFID technology in a wide range of contexts. For the purposes of this Framework, the definitions set out in Directive 95/46/EC should apply regarding privacy and data protection.

The following definitions relate to RFID technology and its Application, and are relevant to the Framework:

Individual. A natural person who interacts with or is otherwise involved with one or more components of an RFID Application (e.g., back-end system, communications infrastructure, RFID Tag), but who does not operate an RFID Application or exercise one of its functions. In this respect, an Individual is different from a User. An Individual may not be directly involved with the functionality of the RFID Application, but rather, for example, may merely possess an item that has an RFID Tag.

Information Security. Preservation of the confidentiality, integrity and availability of information.

Monitor. Carrying out an activity for the purpose of detecting, observing, copying or recording the location, movement, activities, or state of an Individual.

Personal Data. Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

RFID Application. An Application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure.

RFID Application Operator. The natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an Application, including controllers of personal data using an RFID Application.

Radio Frequency Identification (RFID). The use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

RFID Reader. A fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.

RFID Tag or 'tag'. An RFID device having the ability to produce a radio signal or an RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer.

RFID Tag Information or information on the RFID Tag. The information contained in an RFID Tag and transmitted when the RFID Tag is queried by an RFID Reader.

User. Specifically, an RFID Application User, i.e., a person (or other entity, such as a legal entity) who directly interacts with one or more components of an RFID Application (e.g., back-end system, communications infrastructure, RFID Tag) for the purposes of operating an RFID Application or exercising one or more of its functions.

La Prise en Compte de la Vie Privée dans l'Innovation Technologique

Résumé

L'étude de la prise en compte de la vie privée dans l'innovation technologique est celle du régime juridique applicable aux données à caractère personnel. Cependant, la complexité contextuelle du sujet impose une analyse pragmatique, intégrant les éléments économiques et technologiques pour définir l'utilisation effective du droit dans et par l'innovation numérique. Cela passe nécessairement par une approche phénoménologique, expliquant le cheminement juridique qui a conduit le législateur à choisir une telle forme de protection, passant d'un droit au respect de la vie privée général à un régime spécifique applicable aux données à caractère personnel, puis à une observation de son efficacité à protéger l'essence de la vie privée. Au cœur de ce travail se trouve la volonté d'apporter des éléments de réponse objectifs permettant d'expliquer l'écart existant entre la faible confiance du public accordée à la technologie en matière de respect de la vie privée, et les déclarations des législateurs sur l'efficacité des textes protecteurs. Alors que le consentement se trouve être la pierre angulaire du nouveau règlement général sur la protection des données, cette divergence mérite d'être analysée sur un plan juridique. Dès lors, on peut résumer cette thèse à une interrogation: quelle est l'efficacité réelle du régime de protection de la vie privée dans l'innovation technologique ?

Mots clefs français : Droit au respect de la vie privée, Innovation technologique

---

Taking Privacy into Account within Technological Innovations

Abstract

The study of privacy within technological innovations is the study of the legal system surrounding personal data. However, the complexity and context of the subject imposes a pragmatic analysis, gathering elements of economy and technology, to define the reality of the use of the law by and within numerical innovations. As such, it necessitates a phenomenological approach, reviewing the historical steps that lead to the particular set of protections that the legislator has chosen, from a general protection of privacy towards a special regime applicable to personal data, and then an observation of its effectiveness to protect the essence of privacy. At the center of this work, we can find the will to understand the gap between the trust given by the public to technology regarding the respect of one's privacy and the declarations of legislators on the efficiency of the legislative response. Since the consent is the core principle of these regulations, this divergence deserves a legal analysis. Consequently, we can sum this thesis by a simple question: what it the real efficiency of privacy's protection regime facing technological innovations ?

Keywords : Privacy, Technological Innovation

Unité de recherche/Research unit : *Centre d'Etudes et de Recherches Administratives, Politiques et Sociales, 1 place Déliot, 59000 Lille, ceraps@univ-lille2.fr, http://ceraps.univ-lille2.fr/*
Ecole doctorale/Doctoral school : *Ecole doctorale des sciences juridiques, politiques et de gestion, n° 74, 1 place Déliot, 59000 Lille, ecodoc.univ-lille2.fr,* http://edoctorale74.univ-lille2.fr
Université/University : *Université Lille 2, Droit et Santé, 42 rue Paul Duez, 59000 Lille,* http://www.univ-lille2.fr