UNIVERSITE LILLE II
FACULTE DE DROIT

ANNEE UNIVERSITAIRE 2018/2019

MEMOIRE DE RECHERCHE
MASTER 2 DROIT DU TRAVAIL

Maureen ALBIEN

LA PROTECTION DES DONNEES PERSONELLES DES SALARIES A
L'ERE DU RGPD

Directeur de Mémoire :

Monsieur le Professeur des Universités François DUMONT

La Faculté n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions devront être considérées comme propres à leur auteur.

Qu'il soit ici témoigné de ma plus profonde gratitude et remerciements à l'égard,

D'une part, de Monsieur, François DUMONT, Professeur des Universités, pour les précieux conseils et la grande disponibilité dont il a fait preuve à mon égard en répondant invariablement à mes interrogations avec diligence. Ses conseils méthodologiques me suivront.

D'autre part, de l'ensemble des intervenants du Master Droit Social qui, par leurs enseignements, ont largement contribué à la passion que j'ai aujourd'hui pour le droit.

Enfin, de toutes celles et ceux qui m'ont aidé et soutenu pendant mon parcours universitaire. Ils se reconnaîtront.

LA PROTECTION DES DONNEES PERSONELLES DES SALARIES A

L'ERE DU RGPD

SOMMAIRE

Les numéros indiqués renvoient aux pages

Introduction générale	9
1^{ère} partie – L’incidence de la relation de travail sur la protection des données personnelles des salariés	22
Chapitre 1 – L’enjeu de la protection	23
Section 1 – L’assimilation de la protection à la protection de la vie privée du salarié	23
Section 2 – La non-réductibilité de la protection à la protection de la vie privée du salarié ...	33
Chapitre 2 – Les moyens de la protection	46
Section 1 – L’examen de la licéité	46
Section 2 – L’examen de l’effectivité	56
2^{ème} partie – L’incidence du droit des données personnelles sur la protection des données personnelles des salariés	70
Chapitre 1 – La consécration du droit des données personnelles, source de retrait des mécanismes de protection	71
Section 1 – La protection comme exception à la liberté d’entreprendre de l’employeur	71
Section 2 – La protection comme exception à l’objectif de renforcement du Marché intérieur.....	81
Chapitre 2 – La mise en œuvre du droit des données personnelles, source de mutation des mécanismes de protection	92
Section 1 - La libéralisation des mécanismes de protection	92
Section 2 - La contractualisation des mécanismes de protection	104
Conclusion générale	117
Bibliographie	119

Table des matières 131

LISTE DES ABREVIATION

JORF	Journal Officiel de la République Française
AAI	Autorité administrative indépendante
AJDA	Actualité juridique Droit administratif
AJ contrat	Actualité juridique contrat
Art.	Article
C. civ.	Code civil
C.trav.	Code du travail
Cass.	Cour de cassation
C.E.	Arrêt du Conseil d'Etat
CIL.	Correspondant Informatique et Libertés
CNCDH.	Commission Nationale Consultative des Droits de l'Homme
CNIL	Commission Nationale de l'Informatique et des Libertés
Coll.	Collection
D.	Recueil Dalloz
DPD.	Délégué à la protection des données
Dr. ouv.	Droit ouvrier
Dr. soc.	Droit social
Ex.	Exemple
Ed.	Edition
JCP S	Juris-classeur périodique, édition sociale
In	Dans
LIL.	Loi Informatique et Libertés
N°	Numéro

NIR	Numéro de sécurité sociale
NTIC	Nouvelles technologies de l'information et de la communication
Obs.	Observations
Op. cit.	<i>Opere citato,</i>
Préc.	Précité
PUF	Presse Universitaire de France
RGPD	Règlement général sur la protection des données
R.J.S.	Revue de jurisprudence sociale
R.D.T.	Revue de droit du travail
R.D.T civ	Revue trimestrielle de droit civil
R.D.T com	Revue trimestrielle de droit commercial
RFDA	Revue française de droit administratif
Sem. soc. Lamy	Semaine sociale Lamy
Soc.	Arrêt de la chambre sociale de la Cour de cassation
TPE/PME	Très petite entreprise/ Petite et moyenne entreprise
V.	Voir
Vol.	Volume

Introduction

« Le courage, c'est de surveiller sa machine à tisser pour qu'aucun fil ne casse, et de préparer un ordre social plus vaste et plus fraternel, où la machine sera la servante commune des travailleurs libérés.

Le courage, c'est d'accepter les conditions nouvelles que la vie fait à la science et à l'art, d'accueillir, d'explorer la complexité presque infinie des faits et des détails.

Le courage, c'est d'aller à l'idéal et de comprendre le réel »¹.

Si certains auteurs, dont George Orwell, avaient déjà acté, dès le début du 20^{ème} siècle que « le développement de la télévision et le perfectionnement technique qui rend possible, sur le même instrument, la réception et la transmission simultanées, signait la fin de la vie privée »², ils étaient loin d'imaginer l'ampleur qu'allait prendre cette détention d'informations quelques années plus tard face à l'essor du numérique et des nouvelles technologies.

Digne d'une série à rebondissements, les scandales sur la protection des données personnelles (ou plutôt l'absence de protection !) ne manquent pas. De l'affaire « Snowden »³ au scandale « Cambridge Analytica »⁴, en passant par l'affaire « le virus WannaCry »⁵ jusqu'au

¹ Jean Jaurès, Discours à la jeunesse, Albi, juin 1903. Appliqué à la Révolution numérique, le courage est alors d'explorer ce que les nouvelles technologies ont à nous offrir ; c'est d'aller à l'idéal d'un univers connecté et émancipateur et de comprendre le réel c'est-à-dire la complexité et les méfaits que peuvent procurer ces nouvelles technologies.

² G. ORWELL, « 1984 », Trad. Par Amélie Audiberti, Gallimard, Paris, Folio 822.438 p.

³ Les révélations d'Edward Snowden, ex- analyste de sécurité pour un sous-traitant de la NSA, en juin 2013 ont permis de révéler les pratiques américaines sur l'espionnage de masse et la collecte massives d'informations sur les citoyens du monde entier dépassant alors le cadre de lutte nécessaire contre le terrorisme.

⁴ Le scandale « Cambridge Analytica » a permis de révéler la collecte massive de données personnelles d'utilisateurs Facebook. Cette société britannique est accusée d'avoir récupéré illégalement les données personnelles de plus de 50 millions d'utilisateurs du réseau social Facebook. Ces données auraient notamment été utilisées dans le cadre de la campagne de Donald Trump afin d'influencer les électeurs, au travers de publicités et d'opérations de communications ciblées.

⁵ Le scandale « Wannacry » ou « WannaCrypt » fait référence à une attaque informatique ayant touché au moins 300 000 ordinateurs dans 150 pays le 12 mai 2017. Ce logiciel malveillant a exploité une faille de sécurité des systèmes d'exploitation de Microsoft en retard sur leurs mises à jour de sécurité. Le virus informatique a réalisé un chiffrement de données, rendues inaccessibles, et exigé une rançon en Bitcoins pour leur déchiffrement. Ce

simple robot cuiseur de chez Lidl⁶, la sécurisation des données personnelles devient un enjeu majeur à l'ère où la numérisation est reine.

La notion de « données personnelles » est relativement récente. Initialement baptisée « informations nominatives », cette notion concernait les « informations permettant sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent »⁷. Cependant, le manque d'exhaustivité de cette définition a été critiqué. Réduisant la notion aux seules informations comportant le nom, elle ne permettait pas de prendre en compte toutes les informations concernant les individus.

En effet, la loi de 1978 a été rédigée au moment où l'informatique n'en était qu'à ses balbutiements, et où « les dangers provenaient essentiellement des fichiers gouvernementaux pour la création desquels l'intervention humaine était nécessaire, les données étant inscrites manuellement dans la base informatique »⁸. L'avènement et la démocratisation de l'informatique ont changé la donne. Le danger ne provient plus désormais seulement de « l'État mais surtout de toute personne, physique ou morale, détentrice d'un ordinateur. [...] L'information a pu être collectée à distance, de façon automatique, systématique et à l'insu de la personne qu'elle concerne en premier lieu »⁹. Le progrès technologique a donc engendré – à la fois un accroissement quantitatif d'informations concernant les individus par la diversification des procédés de collecte et de traitement de données – mais également un accroissement qualitatif par la multiplication des informations recueillies permettant de « cerner avec plus d'acuité l'individu ».

Ainsi, afin « d'éviter l'obsolescence de la loi, la notion de données à caractère personnel paraissait (...) plus pertinente compte tenu du développement des mesures d'identification indirecte¹⁰. L'« identificabilité » de la personne concernée fait référence « au processus permettant ou aboutissant à sa caractérisation, à sa singularisation, à la révélation de son

virus a infecté des hôpitaux britanniques, ministères russes, des milliers d'entreprises dont le constructeur français Renault.

⁶ L'équivalent du robot-cuiseur Thermomix lancé par Lidl a défrayé la chronique tant les acheteurs se sont rués dans les enseignes pour l'obtenir. Monsieur Cuisine Connect comporte néanmoins quelques failles dont l'existence d'un micro permettant de contrôler la voie mais également de capter les sons environnants. Ce micro dont l'existence n'a pas été renseignée, serait selon l'enseigne « inactivé et inactivable à distance ». Cependant, les risques de détournement de l'objet de ses fonctions à des fins de surveillance ou de chantages informatiques de masse existent, comme en témoignent les nombreux piratages informatiques.

⁷ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF 7 janvier 1978, art 2.

⁸ J. EYNARD, « Les données personnelles : quelle définition, « pour un régime de protection efficace », Paris, Michalon, 2013, 440.

⁹ J. EYNARD, *op. cit.*

¹⁰ Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, JORF n°75 du 29 mars 2014.

identité, ce qui permet de la distinguer des autres personnes physiques »¹¹. Les données d'identification directe sont par excellence les noms et prénoms, l'image ou la voix¹². A contrario, les données d'identification indirectes imposent leur association avec d'autres pour permettre l'identification de la personne. Sont concernées ici les données telles que le numéro de téléphone ou de sécurité sociale, l'adresse géographique ou électronique, la plaque d'immatriculation, les empreintes digitales. L'identifiabilité d'une personne suppose ainsi de détenir un « jeu de données individuelles » permettant de « découvrir l'identité de la personne dans la limite d'un délai, d'un coût et d'une activité raisonnable »¹³.

C'est la loi de 2004¹⁴, transposant la directive communautaire de 1995¹⁵ qui a généralisé l'expression de « données à caractère personnel » ou plus simplement de « données personnelles ». Désormais, est considérée comme une donnée personnelle « toute information relative à une personne physique identifiée ou identifiable (...) ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, 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, psychologique, génétique, psychique, économique, culturelle ou sociale »¹⁶.

Malgré une identité de fond, l'utilisation de la notion de « donnée personnelles » est davantage conforme à la réalité « du fait des évolutions technologiques qui ont été considérables depuis l'élaboration de la loi de 1978 »¹⁷.

Cependant, pour qu'il puisse y avoir identification des individus par le jeu de leurs données personnelles, encore faut-il qu'il y ait un traitement de leurs données.

¹¹ J. POUSSON-PETIT, « L'identité de la personne humaine », *Etude de droit français et de droit comparé*, Bruylant, 2002.

¹² D. HUET-WEILLER, « La protection juridique de la voix humaine », *RTD civ.* 1982, p. 497.

¹³ G. LANG, « Vocabulaire de la statistique et de la protection juridique des données individuelles », *Courrier des statistiques*, n° 107, 2003.

¹⁴ 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 et modifiant la loi n°78-17 du 6 janvier 1978, JO du 7 août 2004.

¹⁵ Dir. 95/46/CE 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, 24 oct. 1995, JOCE du 23 nov. 1995, p. 31, art 4 englobant de façon large « tout ce qui se rapporte à l'identité de la personne, à sa personnalité, à sa vie privée ».

¹⁶ Règl. n° (UE) 2016/679 du Parlement européen et du Conseil, 27 avr. 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, art 4 ; Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n°0288 du 13 décembre 2018, art 2.

¹⁷ J. EYNARD, *op.,cit.*

Un traitement de données à caractère personnel est constitué de « 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, la diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion ainsi que la limitation, l'effacement ou la destruction »¹⁸. Par « limitation de traitement », il faut entendre le marquage de données personnelles concernées, en vue de limiter le traitement futur. Sont donc exclus tous les traitements portant sur des données ne permettant pas l'identification directe ou indirecte des personnes, c'est-à-dire les données anonymes ou ayant fait l'objet d'un processus d'anonymisation¹⁹.

Les données personnelles des salariés font référence, à la fois à leurs données personnelles en tant que citoyen lambda mais également aux données relatives à leur position de subordonné. Or, au sein de l'entreprise, les tâches occasionnant un traitement de données personnelles sont omniprésentes. Elles commencent dès le recrutement avec les données figurant dans les curriculum vitæ des candidats ou collectées lors des entretiens, tests et évaluations. Elles se poursuivent au niveau de l'exécution du contrat de travail avec tout d'abord la gestion des carrières, les évaluations annuelles et professionnelles, la mobilité, allant jusqu'au droit disciplinaire, mais également au niveau de la gestion administrative du personnel avec l'annuaire du personnel sur support informatisé comportant l'identité des salariés, leurs fonctions, leurs coordonnées professionnelles, leur photographie. La paie²⁰ et la politique de rémunération et d'avantages sociaux n'y échappent pas. Les données relatives aux relations sociales sont également concernées notamment celles collectées dans le cadre des élections des représentants du personnel et celles collectées pour la BDES²¹.

D'autre part, les mécanismes relatifs au contrôle du temps de travail et de l'activité des salariés comme les mécanismes de « badgeage » et de vidéo-surveillance ou encore les dispositifs

¹⁸ Règl n°(UE) 2016/679 du Parlement européen et du Conseil, 27 avr.2016, art. 4.2 ; L.n°78-17, 6 janv.1978, art2 mod. par L.2018-493, 20 juin 2018 : JO, 21 juin ; Ordonnance n° 2018-1125 du 12 décembre 2018, art 2.

¹⁹ F. LESAULNIER, « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p.573.

²⁰ Avec le prélèvement à la source, obligatoire depuis le 1^{er} janvier 2019 et effectif depuis cette date, l'employeur traite d'une nouvelle donnée personnelle à savoir le taux d'imposition de son salarié, ce qui suscite de vives réactions. En effet, l'employeur pourrait avoir accès aux revenus du foyer comme notamment la rémunération du conjoint, les revenus liés à leur patrimoine mobilier et immobilier du foyer fiscal. Pour que sa vie privée soit préservée et que ces informations restent confidentielles, le salarié devra retenir le taux non personnalité (ex-taux neutre), indexé uniquement sur son salaire.

²¹ La base de données économique et sociale regroupe l'ensemble des informations relatives aux salariés, aux consultations et informations du Comité société et économique, les indicateurs relatifs à l'égalité professionnelle entre les femmes et les hommes, les écarts de rémunérations, la situation économique, sociale et financière de l'entreprise.

d'alertes professionnelles sont concernés. Enfin, la rupture du contrat de travail implique également le traitement de nombreuses données comme les documents relatifs à la rupture (ruptures conventionnelles, lettres de licenciement) ou encore les documents concernant la fin du contrat de travail.

Le traitement des données personnelles des salariés innervent alors tout le cycle de vie de la relation de travail.

S'interroger sur la définition du droit du travail est nécessaire dans la mesure où l'utilisation des données personnelles n'est admissible qu'au regard d'une activité ou d'une finalité venant légitimer le besoin d'accès aux données. En effet, le droit du travail²² « tend à s'affirmer comme un outil d'organisation, de régulation, et d'épanouissement des activités économiques »²³. La fonction économique du droit du travail prendrait donc le pas sur sa fonction sociale traditionnelle c'est-à-dire la protection de la partie faible au contrat. Cette influence se ressent sur son esprit, lequel « n'est plus seulement de protéger les travailleurs, mais de combiner cette vue avec des exigences économiques ou autres, devenues aujourd'hui si diverses et si pesantes qu'il est de moins en moins possible de tenir à son propos un langage prophétique. Certains n'y ont jamais vu que le droit du capitalisme, d'autres y voient aujourd'hui un droit de gestion des salariés »²⁴. Le droit du travail s'envisage ainsi comme un levier d'action afin d'accroître la productivité, au grand dam de certains²⁵.

Appliqué au droit du travail, il s'agit alors de protéger les données personnelles des salariés à l'égard des traitements opérés par les entreprises.

La notion de protection fait quant à elle référence à l'« action de défendre ou sauvegarder un bien matériel ou immatériel ». La protection implique donc une opération juridique dynamique non statique. Elle suppose ainsi une énergie cinétique. Concrètement, ce caractère dynamique évoque l'idée de choix de la part d'un acteur. La protection des données personnelles se réfère ainsi à une action, un acte positif, un choix, ou encore le comportement d'un auteur pour défendre ses données personnelles contre une utilisation abusive par des tiers. Le silence ou l'inaction de l'acteur ne saurait donc conduire à protéger, de sorte que l'action est une condition.

²² Alors entendu comme « celui qui régit l'ensemble des relations juridiques liées au travail salarié » v. G. COUTURIER, « Droit du travail. Les relations individuelles de travail », Paris, PUF, coll. : Droit fondamental, 3^{ème} éd., 1996, p.15.

²³ B. TEYSSIE, « Droit du travail et droit des affaires », *D.* 2004, p. 2698.

²⁴ J. DEPREZ, « La Cour de cassation », in *Les transformations du droit du travail, Etudes offertes à Gérard Lyon-Caen*, Dalloz, 1989, p. 171.

²⁵ P. LOKIEC, *Il faut sauver le droit du travail !*, Odile Jacob, 2015, p. 17.

La protection des données personnelles des salariés implique donc l'existence de principes et de mécanismes positifs permettant de réguler, au sein de l'entreprise, toutes les opérations se référant à de telles données.

Le droit du travail est donc concerné aussi bien par la protection des données personnelles que par le développement des nouvelles technologies dans la mesure où l'entreprise elle-même y est confrontée. En effet à l'ère de la Révolution numérique, et dans un souci de « performance à outrance », les entreprises ont dû recourir de façon croissante aux outils informatiques et technologiques pour gérer leurs activités puisque celles « qui prétendraient s'y soustraire se placeraient en dehors de la vie sociale telle qu'elle est aujourd'hui organisée »²⁶. Ces nouveaux outils ont pu permettre une nouvelle organisation de l'activité de l'entreprise et une meilleure rationalisation des coûts.

Vue par certains comme des « outils de libéralisation du travail » et « d'émancipation »²⁷, l'utilisation croissante des nouvelles technologies peut être perçue comme contraignante, vecteur de « déshumanisation du travail »²⁸, exposant le travailleur au « fantasme de l'ubiquité »²⁹ mais également fortement intrusive dans la vie privée avec la production d'innombrables données personnelles. Comme tout progrès, des dérives étaient à prévoir. Le risque est que l'entreprise devienne le nouveau « Big brother »³⁰ où l'activité des salariés peut être contrôlée et surveillée en permanence et en toute impunité par l'employeur.

La démocratisation et la généralisation de l'informatique au sein de l'entreprise ont donc eu pour conséquence d'inonder les diverses possibilités de collectes et de traitements de données personnelles des salariés, et a donc soulevé la question de sa compatibilité avec le maintien des droits et libertés fondamentaux, notamment au sein de l'entreprise. Aldous HUXLEY avait ainsi vu juste : « la science est dangereuse, nous sommes obligés de la tenir bien soigneusement enchaînée et muselée »³¹.

Le droit a donc dû intervenir pour appréhender l'utilisation des nouvelles technologies dans l'entreprise « en rendant humainement vivable l'usage de cette technologie »³², tout en

²⁶ JE. RAY, « A propos de la révolution numérique », *Dr.soc.*2012, p.934.

²⁷ J.FRAYSINET, « Nouvelles technologies et protection des libertés dans l'entreprise », *Dr.soc.*1992, p.596.

²⁸ A.SUPIOT, « Fragments d'une politique législative du travail », *Dr. Soc.*, 2011, p.1151.

²⁹ A.SUPIOT, « Travail, droit et technique », *Dr.soc.* 2002, p.13.

³⁰ « Big Brother » fait référence au personnage de fiction issu du roman de Georges Orwell, 1984, désignant un dictateur totalitaire, omniprésent et omnipotent. Désormais, cette expression fait référence à toutes les institutions ou pratiques portant atteintes aux droits et libertés fondamentaux des individus notamment à leur vie privée.

³¹ A.HUXLEY, « Le meilleur des monde », 1932, Pocket Jeunesse, Fantastique, 2001. 285p.

³² A. SUPIOT, *op.cit.*, p.13.

contribuant à son développement pour ne pas freiner l'évolution technologique et ainsi restreindre la compétitivité des entreprises à l'international.

En conséquence, le droit est friand d'instruments juridiques qui promeuvent la protection des données personnelles tout en étant vecteurs de compétitivité. Cette nouvelle ère appelle des instruments de gouvernance propres à concilier la protection des données personnelles des salariés et le principe de la liberté de traitement des données personnelles pour les entreprises. C'est dans cette dynamique qu'intervient le Règlement Européen sur la Protection des Données Personnelles, plus connu sous l'acronyme RGPD³³.

Les évolutions technologiques ont donc nécessairement renforcé le questionnement qui se pose autour de la protection qui doit être accordée aux données personnelles, plus précisément en raison du fait notamment que le rapport entre les évolutions technologiques et la protection des données personnelles fait l'objet d'un saisissement complexe par les différentes branches du droit. Que ce soit en droit du numérique et des nouvelles technologies, en droit de la consommation, des assurances, de la concurrence, c'est un sujet transversal qui transcende toutes les branches du droit. Le droit du travail n'y échappe donc pas. La protection des données personnelles au travail sera ici l'objet de notre étude. L'étude ne portera donc pas sur les traitements de données à des fins archivistiques, scientifiques, historiques ou statistiques³⁴. De même, ne seront pas concernés les traitements de données dans le domaine de la santé ou celles relatives aux condamnations pénales, aux infractions et aux mesures de sûreté connexes³⁵. En effet, seule sera envisagée la protection des données personnelles des salariés dans le cadre de la relation de travail, ce qui exclut la protection de leur donnée non personnelles³⁶.

De même, étant donné que la nouvelle réglementation est applicable à tous les responsables de traitement de données personnelles, les organisations syndicales et le Comité Social et Economique sont également concernés par la nouvelle réglementation. Dès lors, par extension, les règles applicables à l'employeur le seront également pour les syndicats et les représentants du personnel.

³³ Régl.n°(UE) 2016/679 du Parlement européen et du Conseil, 27 avril 2016 entré en vigueur le 25 mai 2018, *op., cit.*

³⁴ *Ibid*, art 89.

³⁵ *Ibid*, art 10.

³⁶ Les données à caractère non personnel sont toutes les données autres que les données personnelles c'est-à-dire toutes les informations ne se rapportant pas à une personne physique ou alors ne permettant pas son identificabilité.

Par ailleurs, dans le cadre de cette étude, les salariés seront envisagés en cette qualité ainsi qu'en leur qualité de citoyen. Aussi, évoquer la première revient à évoquer la seconde.

Enfin, il ne s'agit pas d'analyser uniquement la protection des données personnelles des salariés, mais de mettre en évidence le mouvement d'imbrication du système induit par le RGPD. Dès lors, il paraît évident que l'étude n'aura pas pour objet de recenser la multitude des règles applicables à chaque traitement de données des salariés, mais au contraire de dégager les traits et idées directeurs à la base de la construction du nouveau système. L'étude ne sera donc pas exhaustive dans la mesure où il est inutile de cataloguer les dispositifs de protection applicables à chaque traitement, les guides pratiques de la CNIL étant particulièrement clairs à ce sujet. Par conséquent, l'étude portera sur une analyse des nouvelles logiques induites par le RGPD.

La protection des données personnelles est relativement prégnante. Historiquement, c'est vers les années 1970 que sont apparues les premières mesures visant à encadrer les nouvelles technologies. En 1970, le Land de Hesse en Allemagne avait mis en place une instance indépendante chargée de surveiller les « traitements automatisés des informations nominatives ». Fort de son succès, les autres Lander suivirent l'exemple et une loi fédérale a vu le jour en 1977³⁷. Il n'est pas inutile d'évoquer le « Privacy Act » américain de 1974 dont l'objectif était « d'établir une balance entre les besoins du gouvernement de détenir des informations sur les individus et les droits de ces derniers à être protégés contre les invasions dans la vie privée » même s'il était exclusivement destiné aux fichiers détenus par les administrations fédérales³⁸. Précurseuse, la Suède s'est voulue le modèle à suivre puisque c'est elle qui adopta la première loi nationale de protection des données personnelles en 1973³⁹. En France, le droit à la protection des données personnelles s'est transformé par à-coups. Plusieurs étapes peuvent être identifiées.

Tout d'abord, la première loi de protection de données personnelles, la loi relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » a été adoptée en 1978⁴⁰ pour répondre à la crainte suscitée par le projet SAFARI qui ambitionnait de connecter

³⁷ N.METALLINOS, « La fonction de « détaché à la protection des données » en Allemagne et aux Pays-Bas », *Dr.soc.*2004, p.1066.

³⁸C.CASTETS-RENARD, « La protection des données personnelles dans les relations internes à l'Union européenne », *Dr.soc.* 2018 (actualisation : Mai 2019).

³⁹ M.VIVANT, N.MALLET-POUJOL, « Informatique », Répertoire de droit international, janvier 2019.

⁴⁰ *Ibid.*

l'ensemble des fichiers de l'administration, notamment par le biais du numéro INSEE⁴¹. C'est donc en raison de la crainte d'un éventuel « fichage » des Français, que la loi « Informatique et libertés » est née. En France, c'est donc la loi Informatique et Libertés de 1978 qui a posé les fondements en matière de protection des données personnelles, tout en veillant à ce que l'informatique se développe. L'objectif de cette loi est clairement défini : « 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 »⁴². C'est par cette loi qu'est née la Commission Nationale de l'Informatique et des Libertés (« CNIL »), Autorité administrative indépendante (AAI) chargée d'assurer la qualité du traitement. Cependant, à la date de sa création, le rôle de la CNIL se cantonnait au contrôle des formalités préalables à accomplir auprès d'elle (déclarations et autorisations préalables). Il a fallu attendre 2004 pour que le législateur renforce ses pouvoirs en lui conférant un véritable pouvoir de sanction.

Ensuite, le premier tournant est impulsé par l'Union européenne. Les données personnelles n'étant plus considérées comme un « univers clos »⁴³, les nouvelles technologies ont en effet engendré une multiplication des flux transnationaux. Etant donné que les données personnelles transcendent à la fois les frontières étatiques mais également les frontières inter-spatiales, il est apparu nécessaire qu'existe une réelle collaboration interétatique pour que la protection puisse être efficace. Une harmonisation entre les réglementations nationales en matière de protection était donc souhaitée et nécessaire.

C'est dans cet optique, et consciente que l'utilisation des nouvelles technologies n'est plus l'apanage du secteur public, que l'Union européenne est intervenue au milieu des années 1990 avec l'adoption de la directive 95/46/CE⁴⁴, en imposant une profonde rénovation de la loi « Informatique et libertés » par la loi du 6 août 2004⁴⁵.

Enfin, dernier en date, le RGPD se présente comme apportant un niveau élevé et uniforme de protection des données personnelles tout en attribuant des droits forts aux individus et en garantissant une concurrence loyale à l'ère du numérique. En étant non plus

⁴¹ P. BOUCHER, « SAFARI ou la chasse aux Français », Le Monde, 21 mars 1974. « Code SAFARI » faisant référence au système automatisé pour les fichiers administratifs et le répertoire des individus.

⁴² Loi n° 78-17 du 6 janvier 1978, *op. cit.* art 1.

⁴³ S.FEDAUI, « La protection des données personnelles face aux nouvelles exigences de sécurité », Mémoire Rouen, 2008.

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*, avec six ans de retard sur la date limite de transposition initialement fixée au 24 octobre 1998, ce qui traduisait alors les difficultés du législateur français à reprendre la loi fondatrice et ses réticences à l'égard des objectifs économiques qui sous-tendaient le texte européen.

dans une logique d'harmonisation mais d'uniformisation⁴⁶, ce règlement bouleverse les règles encadrant le traitement des données personnelles dans les Etats membres de l'Union européenne. S'il reprend les principes et les obligations contenues dans la loi de 1978, il met fin aux démarches préalables auprès de la CNIL. D'un contrôle *a priori*, a succédé un contrôle en continu et *a posteriori*. L'idée majeure de ce texte est de responsabiliser les détenteurs de données personnelles en les obligeant à apporter la preuve du respect de la réglementation, sous peine de lourdes sanctions à la fois pénales mais surtout administratives. Les entreprises n'ont donc plus de formalité préalable à effectuer auprès de la CNIL ; ce système est remplacé par un système d'autocontrôle continu et de responsabilisation des entreprises et des sous-traitants.

D'applicabilité directe⁴⁷, ce règlement n'en demeure pas moins très original en laissant plus d'une cinquantaine de « marges de manœuvre » aux Etats membres pour une adaptation du droit interne⁴⁸. Notamment, le RGPD autorise les « Etats membres à prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés, en ce qui concerne le traitement des données à caractère personnel des salariés dans le cadre des relations de travail⁴⁹ ».

Contrairement à l'Allemagne et l'Autriche qui avaient modifié leur législation nationale avant même l'entrée en vigueur du règlement le 25 mai 2018, la « France a adapté la *LIL* hors délai et à la suite d'une procédure accélérée infructueuse : le dépôt tardif du texte le 13 décembre 2017, sans doute repoussé par les échéances électorales, n'a pas facilité les discussions au Parlement »⁵⁰.

Préparée à la hâte, la loi du 20 juin 2018⁵¹ procède à la modification de la loi du 6 janvier 1978, déjà modifiée en partie par la loi « pour une République numérique »⁵². En ne souhaitant pas abroger purement et simplement la loi de 1978, le législateur français a créé de la complexité en produisant l'effet inverse recherché, à savoir l'absence de clarté et de précision et son

⁴⁶ L'uniformisation du droit se présente comme une méthode plus radicale puisqu'à la différence de l'harmonisation, elle a pour objectif d'effacer les différences entre les législations nationales en leur substituant un texte unique, rédigé en des termes identiques pour tous les Etats concernés.

⁴⁷ S.GUINCHARD ET T.DEBARD, « Lexique des termes juridiques », 21^e édition, 2014, Dalloz, p.68. L'applicabilité directe est le fait, pour certains actes communautaires, de « s'appliquer directement dans le droit interne des Etats sans qu'il soit besoin, voire possible, que cet Etat transpose préalablement cette règle dans son droit interne par l'adoption d'une loi ou d'un acte réglementaire ».

⁴⁸ Le Conseil constitutionnel assimile d'ailleurs le RGPD dans son contrôle à une directive v. Cons. const., 12 juin 2018, n° 2018-765 DC, Loi relative à la protection des données personnelles, *AJDA* 2018. 1191.

⁴⁹ *Ibid.*, art 88.

⁵⁰ L. CLUZEL-METAYER ET E. DEBAETS, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101.

⁵¹ Loi n°2018-493, 20 juin 2018 relative à la protection des données personnelles, *JORF* n°0141 du 21 juin 2018.

⁵² Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique, *JORF* n°0235 du 8 octobre 2016.

application imprévisible pour les justiciables⁵³. Son caractère illisible ayant été décrié⁵⁴, l'ordonnance du 12 décembre 2018 permet une remise en forme de la loi « Informatique et libertés » en procédant à sa réécriture.

Fidèle à l'esprit du RGPD, « la loi du 20 juin 2018 embrasse et retranscrit en droit interne le nouvel équilibre issu du RGPD »⁵⁵. En contribuant à la redéfinition du cadre juridique national en matière de protection des données personnelles, la loi entérine notamment la suppression du mécanisme de formalités préalables.

Il n'est pas fortuit de se demander si la question de la protection des données personnelles suscite un intérêt ou devrait en susciter. De fait, entreprendre une étude sur la protection des données personnelles en droit du travail peut paraître a priori dépourvu d'intérêt, tant la pratique de la collecte des données personnelles est omniprésente dans l'entreprise et que l'existence d'un rapport de subordination empêche l'expression de contestation. En plaçant le salarié sous l'autorité de l'employeur, le contrat de travail, par sa nature même, est un « mode de restriction des libertés »⁵⁶. Ce recul du principe de l'autonomie de la volonté se manifeste ainsi en matière de traitement des données personnelles des salariés. Cette omniprésence et l'absence de choix ont conduit à une sorte de banalisation de cette question, voire à l'indifférence des personnes à l'égard de l'utilisation des informations les concernant. Cependant, cette question ne perd pas tout intérêt puisque si le domaine de la protection est méconnu, il est de principe d'annuler la décision illicite fondée sur une exploitation du traitement portant atteinte aux droits et libertés des personnes. Cette annulation, en raison du fait que le traitement outrepassé les règles légales, prend la forme de la nullité et/ou d'une réparation. Si les effets de la nullité, rétroactifs, sont supposés rétablir la situation antérieure à la décision illicite, le droit du travail se prête parfois mal à la « reconstitution » des droits des salariés. Aussi, la nullité ne vaut parfois, en cas d'impossibilité de rétablissement de la situation antérieure, que pour l'avenir et ici seule l'action en réparation ne sera envisageable. De même, la possibilité de sanctions pénales et administratives a suscité l'intérêt, non pas, cette fois-ci, des salariés mais des employeurs.

⁵³ Règl. n° (UE) 2016/679, *op. cit.*, considérant 41.

⁵⁴ Le Conseil d'Etat a considéré la loi comme « économe » et aboutissant à un « résultat très insatisfaisant en termes de lisibilité du droit positif » v. CE, avis, 7 déc. 2017, n° 393836. Le Conseil constitutionnel a quant à lui considéré que la complexité était inhérente au droit européen et a écarté l'argument tenant à la méconnaissance de l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi v. Cons. const., 12 juin 2018, n° 2018-765 DC.

⁵⁵ L. CLUZEL-METAYER ET E. DEBAETS, *Ibid.*

⁵⁶ L. PECAUT-RIVOLIER, Y. STRUILLOU, et P. WAQUET, « Le pouvoir de direction et les libertés des salariés », *LGDJ*, éditeur Liaisons, collection Droit vivant, 2014.

Par ailleurs, le législateur a dû jouer à l'équilibriste en tentant de concilier enjeux économiques et respect des droits des personnes. L'*empowerment* – renforcement des droits des personnes – et l'*accountability* – responsabilisation des acteurs – sont désormais les maîtres-mots du régime protecteur. Le législateur français a dû prendre acte de ce renversement de perspective.

En adaptant ses instruments juridiques à des exigences provenant principalement de l'Union européenne, la France fait œuvre d'une certaine évolution voire d'une « petite Révolution »⁵⁷. En effet, les fondements du système français en matière de données personnelles ont été métamorphosés. Cependant, même s'il y a une remise en cause du système, il s'avère qu'elle ne peut être qualifiée de véritable Révolution puisque l'objectif poursuivi, même s'il a été accentué, est resté identique : assurer la liberté de circulation des données en « contribuant à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien être des personnes physiques »⁵⁸. Ces paroles qui n'ont pas seulement une beauté philosophique permettent de comprendre que la protection des données devra être mise en balance avec la liberté d'entreprendre notamment la liberté de traitement des données personnelles. Ainsi vecteur de progrès, le développement de la protection des données personnelles est fonction de la place que les politiques publiques européennes entendent lui donner.

Une opposition entre le principe de la liberté des traitements de données personnelles et la protection desdites données s'installe. Il aurait pu paraître pertinent de bâtir le plan de notre recherche en divisant ces deux idées : d'une part la liberté de traitement des données induite par les exigences propres à l'employeur et d'autre part les mécanismes de protection des salariés à l'égard de ces traitements. Cependant il n'est pas possible de distinguer clairement ces deux idées en deux parties sans empiéter dans l'une en évoquant l'autre puisque ces deux idées se trouvent disséminées à tous les stades du traitement de données personnelles, c'est-à-dire dès la mise en place de la collecte jusqu'à la destruction de ces dernières, en passant bien évidemment par leurs exploitations. Une autre division devait s'opérer.

Appliquée à la relation de travail, la protection des données personnelles des salariés connaît une relation ambivalente. L'employeur étant perçu comme collecteur et générateur de nombreuses données personnelles, le droit du travail apparaît comme le « bouclier et l'épée » de la protection des données personnelles des salariés. Toutefois, le « nouveau droit des

⁵⁷ P.BLOUM, « Le RGPD, révolution ou évolution », *Lextenso*, Petites affiches – n°126, juin 2018.

⁵⁸ Règl. n° (UE) 2016/679, *op. cit.*, art 1.

données personnelles », issu du nouveau paradigme induit par l'entrée en vigueur du RGPD⁵⁹, est susceptible de constituer une menace pour la protection des données personnelles des salariés tant le modèle traditionnel de protection s'en trouve bouleversé. Dans ce contexte, se pose la question du caractère « illusoire » ou, à tout le moins, dérisoire de l'efficacité des mécanismes relatifs à la protection des données personnelles.

L'évolution des instruments juridiques en matière de protection des dites données suscite l'hypothèse de recherche suivante.

Par cette étude, nous tenterons de démontrer que si le droit des données personnelles est traditionnellement envisagé comme un droit offrant une protection des citoyens-salariés à l'égard des traitements de leurs données personnelles, cette protection est résiduelle et le principe se trouve désormais dans le nouveau droit des données personnelles issu du RGPD, au service de la mondialisation et du droit post-moderne.

Deux temps vont guider notre démonstration.

Le traitement des données personnelles dans l'entreprise, envisagé comme outil de gestion de l'activité et de surveillance des salariés, a connu un large développement depuis sa reconnaissance. En étant synonyme d'accroissement des risques d'atteintes aux droits et libertés fondamentaux des salariés, il est apparu nécessaire d'assurer une protection. La relation de travail, caractérisée par la subordination du salarié envers son employeur, a alors des répercussions sur la protection des données personnelle des salariés (Partie 1).

Confrontée au changement de paradigme induit par le RGPD, le sort de la protection des données personnelles des salariés soulève des interrogations. La consécration du nouveau droit des données personnelles pourrait sembler y porter l'estocade, bien qu'une autre analyse conduise à relativiser l'incidence de ce nouveau droit sur la protection des données personnelles des salariés (Partie 2).

⁵⁹ L. CLUZEL-METAYER ET E. DEBAETS, *op.,cit.*

PARTIE I

L'INCIDENCE DE LA RELATION DE TRAVAIL SUR LA PROTECTION DES DONNEES PERSONNELLES DES SALARIES

La révolution numérique a pénétré les portes de l'entreprise. Cette révolution n'est pas sans conséquences sur la relation de travail tant il est fréquent qu'elle impose de recueillir et de traiter des données personnelles des salariés. Permettant d'accroître l'enrichissement des entreprises par l'accélération du processus de production, la pénétration du progrès numérique et technologique, dans et hors l'enceinte de l'entreprise, sert également de moyen de contrôle sur l'environnement virtuel⁶⁰ et réel⁶¹ du salarié.

Hypertrophiques, ces dispositifs de traitement ont montré leurs écueils à assurer de manière paisible la protection promise aux salariés.

Etant donné que le salarié est placé sous la subordination de son employeur, et que de son contrat de travail dépend sa rémunération, il est apparu indéniable de protéger les données personnelles du salarié. A cet effet, en affinant l'analyse de l'enjeu de la protection (Chapitre 1), il conviendra de s'intéresser aux moyens mis en place dans le cadre de la protection, qui voient un nouvel ordre se dessiner (Chapitre 2).

⁶⁰ Au travers l'outil informatique (matériels informatiques de l'entreprise mis à la disposition du salarié), Internet (connexion Internet, réseaux sociaux), les communications électroniques ou téléphoniques du salarié.

⁶¹ Au travers des dispositifs de vidéo-surveillance, biométriques, de géolocalisations, d'enregistrement sonore.

Chapitre I – L’ENJEU DE LA PROTECTION

Si le droit à protection des données personnelles n’a jamais fait l’objet d’une consécration constitutionnelle, la fondamentale de ce droit a en revanche été reconnue par l’article 8 de la Charte des droits fondamentaux de l’Union européenne⁶², puis confirmée par le considérant 1 du RGPD⁶³.

Permettant de protéger la personne humaine des traitements de données personnelles la concernant, la protection des données du même nom concourt à la protection de la vie privée (A). Cependant, n’envisager sa protection qu’à l’aune de la vie privée est réducteur. La protection dépasse ce seul champ et touche d’autres droits fondamentaux (B).

Section 1 – L’assimilation de la protection des données personnelles à la protection de la vie privée

Si le droit interne⁶⁴ et européen⁶⁵ originels ont pris en compte l’impact du développement numérique et technologique sur la vie privée des individus, les Etats sont désormais confrontés à une certaine Révolution numérique qui a multipliée par 1000 les capacités de stockages, de traitements et de circulations des informations⁶⁶. En envahissant tous les champs de la vie sociale, la notion traditionnelle de la vie privée dans l’entreprise est apparue inadaptée et a dû évoluer (A) jusqu’à être transformée par l’avènement de l’homo numericus (B)

§1. L’évolution de la vie privée à l’âge de l’ « homo sapiens »

La multiplication des dispositifs de traitement, à même de prélever et de conserver de nombreuses données personnelles des salariés, occasionne une « perméabilisation croissante entre la frontière vie privée et vie publique du salarié »⁶⁷. En subissant une profonde évolution,

⁶² Article 8 de la Charte des droits fondamentaux de l’Union européenne du 7 décembre 2000 : « Toute personne a droit à la protection des données à caractère personnel la concernant ».

⁶³ Règl. n° (UE) 2016/679, *op. cit.*, considérant 1 prévoyant que « la protection des personnes physiques à l’égard du traitement des données à caractère personnel est un droit fondamental ».

⁶⁴ Loi n° 78-17 du 6 janvier 1978 *op. cit.*

⁶⁵ Directive 95/46/CE du 24 octobre 1999, *op. cit.*

⁶⁶ Avis du 22 mai 2018 sur la protection de la vie privée à l’ère du numérique, *JORF* n°0126 du 3 juin 2018 texte n° 63.

⁶⁷ M.PEYRONNET, « La vie privée du salarié sur internet en voie d’extinction », *Dalloz actualités*, 29 janvier 2016.

la notion civiliste de vie privée n'est alors plus parue pertinente. La notion travailliste de vie personnelle du salarié est donc née⁶⁸ et a entraîné avec elle le passage de la protection traditionnelle du cercle intime du salarié (A) au cercle personnel de ce dernier (B).

A. La protection traditionnelle au cercle intime du salarié

La notion de « droit au respect de la vie privée » fait l'objet d'un rayonnement international. Envisagée pour la première fois par la Déclaration universelle des droits de l'homme des Nations unies⁶⁹, elle a ensuite été reprise par de nombreux textes internationaux et européens⁷⁰. En droit interne, cette notion est relativement récente⁷¹ et a pour siège textuel l'article 9 du Code civil prévoyant que « chacun a le droit au respect de sa vie privée ». Elevée au rang de droit fondamental⁷², la protection de la vie privée, garantie par le droit au respect de la vie privée est historiquement une notion civiliste ne bénéficiant qu'aux citoyens de la cité. Cependant en devenant « citoyen de la Cité » mais également « citoyen dans l'entreprise »⁷³, les travailleurs se sont vus reconnaître le droit au respect de la vie privée. Cette reconnaissance est apparue nécessaire afin de « soustraire de l'emprise de l'employeur un aspect important de la personne » du salarié⁷⁴.

Cette reconnaissance universelle allait donc nécessairement se retrouver dans les textes originels⁷⁵ mais également dans la nouvelle loi « Informatique et Libertés »⁷⁶ issue du RGPD. L'objectif est de prévenir toute ingérence potentielle de l'employeur dans la vie privée des salariés. Or, la gestion de l'activité des salariés par la mise en place de dispositifs de traitements des données personnelles précités peuvent venir troubler leur droit au respect de la vie privée.

⁶⁸ P. WAQUET, « La vie personnelle du salarié », *Dr.soc.*, 2004, p.23.

⁶⁹ Déclaration universelle des droits de l'homme des Nations unies du 10 décembre 1948, article 12 : « nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation [...] ».

⁷⁰ Article 8§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales admet que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». La protection de la vie privée a aussi été reconnue par la Convention américaine des droits de l'homme adoptée en 1969, en son article 11.

⁷¹ Loi n°70-643 du 17 juillet 1970, JORF 19 juillet 1970, art 22.

⁷² Cons.const., 23 juill. 1999, n°99-416, DC, JO 28 juill.1999.

⁷³ P. WAQUET, « Vie privée, vie professionnelle et vie personnelle », *Dr.soc.*, 2010, p.14.

⁷⁴ O. DE TISSOT, « La protection de la vie privée du salarié », *Dr.soc.*, 1995, p. 222.

⁷⁵ Directive 95/46/CE, *op.cit.*, art 1^{er} : l'objectif de cette directive tend à « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel ».

⁷⁶ Loi n°2018-493, 20 juin 2018, *op.cit.*, art 1 : « l'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles dans l'entreprise ».

La protection de la vie privée du salarié revêt donc une importance particulière. Cependant, il n'existe pas de définition formelle de la vie privée. Le RGPD, ni même le Code civil, n'ont pris le soin d'établir une définition unique puisque « la notion de vie privée est une notion large, non susceptible d'une définition exhaustive »⁷⁷. Cette économie de définition fait de la notion de vie privée un standard juridique qu'il appartient aux Etats et aux juges de modeler au gré des évolutions de la société.

Pour tenter d'y apporter une définition, il convient de se rapporter au « right of privacy » américain qui définit la vie privée comme « la sphère de la vie où l'individu aura le pouvoir d'écarter des tiers »⁷⁸. Le droit au respect de la vie privée correspond donc pour tout individu, y compris dans les relations de travail⁷⁹, au « droit de se masquer »⁸⁰ et d'écarter de sa sphère intime toute intrusion de tiers non consentie. C'est parce que les données personnelles du salarié, générées par les dispositifs de traitements précités, peuvent avoir un impact sur la vie professionnelle du salarié tant au niveau du recrutement (refus d'embauche), de l'exécution (refus d'octroi de promotion/primes) que de la rupture du contrat de travail (perte d'emploi injustifiée en raison de faits relevant de la vie privée du salarié) qu'il convient de préserver le salarié d'une intrusion de l'entreprise dans sa sphère d'intimité.

L'exemple du domicile est révélateur. Considéré comme le sacro-saint lieu de l'intimité de la vie privée, l'adresse postale liée au domicile « joue sur les deux tableaux » en étant à la fois une donnée intime et une donnée personnelle du salarié. Aussi fait-elle montre des liens qu'entretiennent vie privée et données personnelles.

Attachée au domicile, l'adresse IP suit le même sort⁸¹ : elle fait l'objet d'une protection conjuguée d'une part au titre de la protection de la vie privée et d'autre part, au titre de la protection des données personnelles, ce qui ne manque pas de révéler davantage une certaine identité entre les deux protections.

Le développement massif des services numériques et technologiques a toutefois révélé l'inefficacité de la conception traditionnelle à protéger l'intégralité de la vie privée du salarié,

⁷⁷ CEDH, 19 septembre 2013, Von Hannover c/Allemagne, n°8772/10, CEDH 2013.

⁷⁸ J.CARBONNIER, « Droit civil », volume 1, Paris : PUF, 2004, p. 518.

⁷⁹ Cass., 1^{re} Civ. 23 octobre 1990, n° 89-13.163, Bulletin 1990 n° 222 : « Toute personne, quels que soient son rang, sa naissance, sa fortune, ses fonctions présentes ou à venir, a droit au respect de sa vie privée ».

⁸⁰ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *art., préc.*

⁸¹ Cass, 1^{ère} ch. civ., 3 novembre 2016, n°15-22.595 : « Les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL ». La Cour de cassation s'inscrit alors dans la jurisprudence de la Cour de justice de l'Union européenne (CJUE, 19 oct. 2016, Patrick Breyer c/ Bundesrepublik Deutschland, aff. C-582/14, D. 2016. 2215).

commandant ainsi son dépassement. Ce développement, notamment au travers d'Internet et des réseaux sociaux, a rendu la démarcation entre vie privée et vie publique difficile. Puisque chaque salarié en tant qu'individu partage, consciemment ou non, de nombreuses informations les concernant, faisant d'éléments ordinairement privés, des données pouvant être connues par les entreprises, le rattachement à la seule protection de la vie intime du salarié s'est avéré réducteur et imparfait.

Une extension de la protection devait donc s'opérer pour s'adapter davantage à l'univers technologique et aux traitements de données personnelles dans l'entreprise. La jurisprudence travailliste inventa alors la notion de vie personnelle. Cette notion constitue un instrument utile au regard du droit à la protection des données personnelles.

B. La protection extensive au cercle personnel du salarié

Distincte de la vie privée, la notion de vie personnelle est une notion prétorienne forgée par et pour les relations de travail.

La notion de vie personnelle a vu le jour en 1980 dans la jurisprudence de la Chambre sociale de la Cour de cassation. Tout d'abord employée dans le cadre du contentieux de la protection sociale comme la négation de la vie professionnelle⁸² - c'est-à-dire le temps pendant lequel le salarié n'était pas au travail - elle fut ensuite évoquée dans le contentieux du droit du travail concernant une sanction disciplinaire ne pouvant en principe pas reposer sur un fait tiré de la vie personnelle du salarié⁸³. Par extension, les données personnelles faisant référence à la vie personnelle du salarié suivent le même régime.

Le changement terminologique a son importance notamment dans son rapport avec la protection des données personnelles. En effet, puisque certains faits accomplis par le salarié en dehors du temps et lieu de travail – donc en dehors de l'autorité de l'employeur – ne relèvent pas stricto sensu de l'intimité de sa vie privée puisqu'ils s'exercent au grand jour, il a fallu

⁸² Cass. soc. 17 Mai 1982 n° 80-16.541.

⁸³ Cass. soc. 9 décembre 1992 n° 89-42.547 à propos d'une clause de mobilité géographique d'une salariée « qui mettait celle-ci dans l'impossibilité de concilier sa vie personnelle et ses obligations professionnelles » puisque la mutation était intervenue le jour de la rentrée scolaire de son fils. La chambre sociale de la Cour de cassation rejeta pourtant ce moyen, considérant que la mise en oeuvre de la clause n'était pas discriminatoire. ; Cass. soc. 14 Mai 1997 n° 94-45.473: Ce n'est que quelques années plus tard que la chambre sociale de la Cour de cassation a admis que « les agissements du salarié dans sa vie personnelle n'étaient pas constitutifs d'une cause de licenciement ». En l'espèce, un gardien d'immeuble a été licencié pour faute lourde pour avoir eu une altercation avec un locataire de la résidence dans laquelle il était employé. L'altercation s'étant produite pendant son congé maladie, les faits se sont produits en dehors de la vie professionnelle du salarié. Le licenciement était donc dépourvu de cause réelle et sérieuse.

revoir la protection à l'heure où « l'exposition de soi » sur les réseaux sociaux est dans l'air du temps. A titre d'illustration, l'activité associative, religieuse, politique et syndicale⁸⁴ relève de la vie personnelle du salarié.

En recouvrant trois aspects, « la vie privée proprement dite, l'exercice des libertés civiles (mariage divorce) et l'exercice des libertés civiques (participation à la vie politique et associative) »⁸⁵, la protection de la vie personnelle du salarié permet de protéger au-delà du simple cercle intime et d'y inclure des éléments connus des tiers dans son cercle de protection. De nombreuses données personnelles sont donc concernées puisque sont visées ici toutes les données de géolocalisation et toutes les données collectées et diffusées sur Internet et les réseaux sociaux.

En élargissant le spectre de protection du citoyen-salarié pour le faire correspondre au développement du numérique, la jurisprudence a eu conscience des risques que peuvent provoquer ces nouvelles technologies, par la captation en masse de données personnelles, sur la vie personnelle du salarié. Ainsi si la protection de la vie privée est plus restreinte que celle relative à la vie personnelle, elle est également plus large puisqu'elle s'applique non exclusivement aux salariés, mais à tous les citoyens. La vie personnelle est par conséquent la forteresse dont la vie privée serait le donjon⁸⁶.

Par conséquent, en assurant la protection de la vie personnelle du salarié, la protection des données personnelles permet de faire échapper une partie de la vie du salarié au lien de subordination caractérisant le contrat de travail⁸⁷. En ce qu'elle constitue « beaucoup plus un vecteur du contrôle de l'autorité patronale qu'une réplique partielle des droits fondamentaux de la personne »⁸⁸, la notion de vie personnelle est donc l'une des bornes générales du pouvoir de l'employeur. Elle permet donc au salarié d'être préservé, pour des faits extérieurs à la vie professionnelle ne relevant pourtant pas de la vie privée, de l'influence du pouvoir disciplinaire de l'employeur.

Encore une fois, à l'image du constat effectué à propos de la conception traditionnelle de la vie privée, protection de la vie personnelle et protection des données personnelles agissent de concert afin de prémunir le salarié d'ingérences illicites de l'employeur.

⁸⁴ G.LOISEAU, « Focus sur la vie personnelle du salarié », D. 2009, p.2393.

⁸⁵ J. RICHARD DE LA TOUR, « La vie personnelle du salarié. Étude sur la jurisprudence récente de la chambre sociale de la Cour de cassation », Rapport annuel de la Cour de cassation pour l'année 1999.

⁸⁶ P. WAQUET, « La vie personnelle du salarié », *Dr. soc.* 2004, p. 25.

⁸⁷ F.FAVENNEC-HERY, « Vie professionnelle, vie personnelle du salarié et droit probatoire », *Dr.soc.* 2004, p. 48.

⁸⁸ A. LYON-CAEN ET I.VACARIE, « Droits fondamentaux et droit du travail », *Mélanges en l'honneur de J. M. Verdier, Dalloz*, 2001, p. 421.

En définitive, « lorsqu'il s'agit de faire respecter la personne du salarié, la conception de la vie privée a été mise au format, plus ample, de la vie personnelle »⁸⁹. La notion de vie privée n'est donc pas une notion figée. Cette notion a évolué, ce qui a permis au salarié d'être protégé, à la fois dans son cercle intime et personnel. Si cette notion a évolué, elle s'est également transformée au regard de la place qu'a pris la « société de l'information »⁹⁰ sur le quotidien des salariés. Le salarié étant devenu un homo numericus⁹¹, les ambitions tenant à la protection allaient redessiner le concept de vie privée.

§2. La transformation de la vie privée à l'âge de l' « homo numericus »

En devenant une espèce connectée en permanence, l'homo sapiens est devenu un homo numericus⁹². La Révolution numérique n'est pas sans importance sur la capacité de l'humain à décider de lui-même. Une certaine forme d'aliénation par le numérique se ressent sur l'autodétermination de l'individu.

Appliquée à la relation de travail, si le salarié accepte par avance une perte d'autonomie puisqu'il est placé sous la subordination, voire sous la dépendance économique d'un employeur⁹³, il doit toutefois garder une part de son autodétermination. Face à une « société de l'information » guidant de plus en plus les décisions des citoyens-salariés, comme en témoigne le nombre florissant de ciblage publicitaires à travers les redoutables « cookies »⁹⁴, la protection du droit à l'autodétermination du salarié devenu homo numericus est double : elle est à la fois synonyme d'autonomie décisionnelle (A) et informationnelle (B).

⁸⁹ G.LOISEAU, « Droit civil et droit du travail : une relation instable », *Dr.soc.2019*, p.477.

⁹⁰ La société de l'information, notion apparue dans les années 1990, désigne une société dans laquelle les NTIC jouent un rôle central puisqu'ils permettent, grâce à l'informatique de numériser les informations de façon dématérialisée. La société de l'information fait référence « aux données, aux canaux de transmission et aux espaces de stockage de l'information ». La journée mondiale de la société de l'information a lieu tous les 17 mai selon l'adoption par l'Assemblée Générale de l'Organisation des Nations Unies de la résolution A/RES/60/252. Ainsi selon A.MEBTOUL, « le monde est devenu une grande maison de verre, un acquis contre les régimes totalitaires dans la mesure où l'information n'est plus le quatrième pouvoir mais le pouvoir lui-même ».

⁹¹ G.LOISEAU et A.MARTINON, « L'Homo Numericus », *Les Cahiers Sociaux*, n°290, p.519.

⁹² A.ASTAIX, « Internet : une loi contre les atteintes à la vie privée », *D.* 2010, p.756.

⁹³ M-C ESCANDE-VARNIOL, « Un ancrage stable dans un droit du travail en mutation », *D.* 2019, p.77.

⁹⁴ L-M AUGAGNEUR, « Vers des nouveaux paradigmes du droit dans l'économie numérique », *RTD com.* 2015, p.455. Les cookies sont des traceurs déposés directement sur l'ordinateur d'un individu en fonction du site qu'il a visité. Grâce à ces cookies, les sites internet peuvent identifier les différentes pages Internet qu'il a visitées et créer un historique de navigation. Ils ont notamment pour finalités le ciblage publicitaire c'est-à-dire d'analyser le comportement et les habitudes de consommation d'un individu pour lui proposer notamment des publicités ciblées pour le pousser à la consommation.

A. La protection du droit à l'autodétermination décisionnelle du salarié

La notion d'autodétermination décisionnelle fait référence à la capacité du salarié de décider librement de la conduite qu'il doit adopter. En influençant les choix de vie du salarié par l'accroissement de « l'infobésité », la révolution numérique a eu un impact considérable sur l'autodétermination décisionnelle du salarié.

Impulsée par la jurisprudence de la Cour européenne des droits de l'homme, le concept de vie privée s'est transformé. Il y inclut désormais le droit pour toute personne de librement se construire, se développer personnellement et s'épanouir dans ses relations sociales⁹⁵ ainsi que d'être soi-même en révélant son identité d'être humain⁹⁶.

Cette conception étendue de la vie privée, entendue comme une protection du droit à l'autodétermination du salarié, a conduit certains auteurs à parler de l'avènement d'un droit à une « vie privée sociale ». Selon cette conception, en passant du secret à la vie privée à la liberté dans sa vie privée, « l'individu revendique son autodétermination et entend faire respecter ses choix de vie par la société »⁹⁷. Ainsi, « le droit d'être laissé seul et de tenir au secret certaines informations a laissé la place à la liberté d'exprimer sa vraie personnalité pour parvenir à l'épanouissement personnel »⁹⁸.

Selon cette conception, protéger la vie privée du salarié permet de le protéger contre l'impact que pourrait avoir la divulgation d'informations personnelles sur son intégration dans la société. Ici n'est donc pas visé le comportement individuel de l'employeur à l'égard de son salarié mais bien l'impact que peut causer cette révélation d'informations sur l'intégration sociale du salarié à la fois dans l'entreprise et en dehors.

A cet égard, l'employeur doit donc s'abstenir de communiquer à des tiers des données personnelles relatives aux revenus professionnels des salariés, et ce même si cette communication ne leur est pas préjudiciable⁹⁹.

⁹⁵ CEDH, *Pretty c/ Royaume-Uni*, 29 avril 2002, req. n°2346/02.

⁹⁶ CEDH, *Christine Goodwin c/ Royaume-Uni*, Grande chambre, 11 juillet 2002, req. n° 28957/95.

⁹⁷ A.BAREGE ET B.BOSSU, « Les TIC et le contrôle de l'activité du salarié », *JCP S* n°41, 8 oct. 2013, p.1393.

⁹⁸ *Ibid.*

⁹⁹ Arrêt CJUE « *Österreichischer Rundfunk* » du 20 mai 2003, e.a., C-465/00, C-138/01 et C-139/01 : « si la simple mémorisation par l'employeur de données nominatives relatives aux rémunérations versées à son personnel ne saurait, comme telle, constituer une ingérence dans la vie privée, la communication de ces données à un tiers, en l'occurrence une autorité publique, porte atteinte au respect de la vie privée des intéressés, quelle que soit l'utilisation ultérieure des informations ainsi communiquées, et présente le caractère d'une ingérence au sens de l'article 8 de la CEDH (...) Pour établir l'existence d'une telle ingérence, il importe peu que les informations communiquées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence. Il suffit que les données relatives aux revenus perçus par un travailleur ou un pensionné aient été communiquées par l'employeur à un tiers ».

Si la révélation des revenus professionnels peut paraître superflue, la protection des données personnelles permet au salarié de ne pas être stigmatisé et ainsi être « marqué au fer rouge » indéfiniment. Cette absence de stigmatisme lui permet d'exercer sa capacité décisionnelle. Or, en étant contraint, cette dernière est nécessairement affectée par la position de subordonné du salarié. Appliquée à la relation de travail, cette contrainte peut être explicite ou implicite.

Dans le premier cas, la capacité décisionnelle du salarié est directement liée à l'emprise de l'employeur sur ce dernier. Concernant cette emprise, le Groupe de travail sur l'article 29 a révélé que si en « théorie le travailleur peut refuser de donner son consentement » à la mise en ligne de sa photographie sur le site internet de l'entreprise, « il peut alors perdre une opportunité d'emploi »¹⁰⁰ La contrainte est ici le risque de ne pas être recruté.

Dans le deuxième cas, la capacité décisionnelle du salarié est directement liée à la connaissance par ce dernier de son environnement de travail. D'une part, les dispositifs de surveillance introduits au sein de l'entreprise affectent la capacité décisionnelle du salarié en le poussant à agir comme un automate. La contrainte est ici le risque de s'exclure des formalismes de travail voire le risque d'être sanctionné en cas d'erreur. D'autre part, le Conseil constitutionnel a reconnu que la réintégration d'un salarié qui a été amnistié « pouvait affecter la liberté personnelle de l'employeur et de ses salariés de l'entreprise en leur imposant la fréquentation, sur les lieux de travail, des auteurs d'actes dont ils ont été victimes »¹⁰¹. La contrainte sera ici le risque d'affecter l'environnement de travail en imposant la présence dudit salarié alors que cette dernière n'est pas souhaitée.

En définitif, en protégeant le salarié d'une atteinte à ses données personnelles, le droit permet implicitement à ce dernier d'exercer pleinement son épanouissement et développement personnels dans ses relations sociales.

C'est donc en protégeant les données personnelles des salariés que la composante décisionnelle de l'autodétermination est préservée.

Cependant le développement des réseaux sociaux et au-delà de l'ensemble des outils mis à la disposition des salariés, dans et hors l'entreprise, leur permettant de partager des informations diffuses, menace également la composante informationnelle de cette

¹⁰⁰ Avis du G29 n° 15/2011 (WP187) du 13 juillet 2011 sur la définition du consentement.

¹⁰¹ Cons.const., 20 juillet 1988, n°88-244 DC.

autodétermination. Cette menace offre un nouveau défi à la réglementation « Informatique et libertés » qui est de préserver le salarié de la diffusion d'informations le concernant.

B. La protection du droit à l'autodétermination informationnelle du salarié

D'origine prétorienne, le droit à l'autodétermination informationnelle a été reconnu pour la première fois par la Cour constitutionnelle fédérale d'Allemagne qui soulignait que « la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel »¹⁰².

C'est donc en permettant au salarié homo numericus de contrôler la captation d'informations réalisées à son égard que ce dernier pourra « vivre une existence ne fut-ce que partiellement autodéterminée » étant donné que « la maîtrise des données personnelles constitue donc une condition de la liberté et de l'épanouissement de l'individu, autant dans sa vie économique que dans sa participation à la cité »¹⁰³.

La promotion récente de ce principe par le Conseil d'Etat¹⁰⁴ et sa consécration dans la nouvelle loi « pour la République numérique »¹⁰⁵, puis dans sa nouvelle loi « Informatique et Libertés »¹⁰⁶ montrent l'intérêt et l'importance du recours à un tel principe.

L'accroissement des traces des données personnelles occasionné par la révolution numérique, associé au développement de l'exposition de soi sur Internet, a étendu l'enjeu de la protection. Désormais l'enjeu n'est plus seulement de protéger les citoyens-salariés contre les traitements de données opérés par les entreprises, mais également de les protéger contre eux-mêmes¹⁰⁷, notamment lors de leurs propres publications compromettantes sur les réseaux sociaux. Par ailleurs, il s'agit également de les prémunir contre les parutions faites par des tiers qui peuvent,

¹⁰² Cour. Constit. Féd. All., 15 déc. 1983, Volkszählungsurteil, BVerfGE Bd. 65, S. 1 ff.

¹⁰³ L-M AUGAGNUR, *art., préc.*, p.455.

¹⁰⁴ Conseil d'État, *Le numérique et les droits fondamentaux*, La Documentation Française, 2014, p. 154 : « face à l'explosion des usages des données personnelles et des risques associés, il faut en repenser la protection et repenser le lien entre protection des données personnelles et autodétermination informationnelle (...) le développement sans précédent du numérique comporte des risques que les personnes concernées ne sont pas en mesure de maîtriser ».

¹⁰⁵ Loi n° 2016-1321 du 7 octobre 2016, *op., cit.*

¹⁰⁶ Loi n°2018-493,20 juin 2018, *op.,cit.*, art 1 : « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données personnelles le concernant ». Le rattachement du droit à la protection des données personnelles à la notion d'autodétermination informationnelle n'est fait qu'implicitement.

¹⁰⁷ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *art., préc.*

en utilisant la technique du « tag »¹⁰⁸, transformer une photo en « objet requêtable et indexable sur un moteur de recherche »¹⁰⁹, rendant la photo « plus visible car plus accessible »¹¹⁰.

Le RGPD s'est donc efforcé de promouvoir cette nouvelle ambition¹¹¹ en assurant aux individus une certaine « hygiène numérique » et en les incitant à cloisonner leur identité numérique et faire régulièrement leur propre veille numérique sur eux-mêmes.¹¹² Les risques sont en effet présents puisque par exemple si la collecte de données sensibles comme l'orientation sexuelle d'un salarié est interdite, elle devient connue dès que le salarié l'a rendu lui-même publique. Or en 2015, 35% des recruteurs reconnaissent avoir écarté un candidat à un emploi en raison des traces qu'il a laissées sur les réseaux sociaux¹¹³. Si ces considérations sont interdites, il n'empêche qu'un recruteur peut être influencé par la connaissance d'informations concernant un candidat puisqu'il ne faut pas oublier qu'un contrat de travail est conclu *intuitu personae* – c'est-à-dire en considération de la personne. Ce constat a même occasionné la création de plateformes « e-réputation » offrant des prestations de service de « nettoyage » de l'identité numérique d'un individu¹¹⁴.

Certains auteurs dont Nathalie Martial-Braz déplorent cependant, l'absence, dans le RGPD, de dispositions formelles reconnaissant un tel principe, alors même que celles-ci étaient pourtant fort attendues. Elle déplore « la timidité du législateur européen, surtout si l'on compare avec la relative témérité du législateur français qui après moult hésitations a fini par admettre implicitement un tel principe »¹¹⁵.

En définitive, force est de constater que la protection de la vie privée à l'ère RGPD laisse de côté les aspects du développement et de l'épanouissement personnels des citoyens-salariés. Ce faisant, le législateur a oublié d'intégrer au régime applicable aux données personnelles la

¹⁰⁸ Le « tag » permet d'associer un nom à une photo par exemple.

¹⁰⁹ N.OCHOA, « Le droit des données personnelles, une police administrative spéciale »Thèse, Paris I, 2014, p.479.

¹¹⁰ *Ibid.*

¹¹¹ Règl. n° (UE) 2016/679 *op., cit.*, considérant 6 : « l'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données personnelles. L'ampleur de la collecte et du partage de données personnelles a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données personnelles comme jamais auparavant dans le cadre de leurs activités (...) Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant ».

¹¹² G.DESGENS-PASANAU, « La protection des données personnelles, le RGPD et la loi française du 20 juin 2018 », *Lexisnexis*, 4^e édition, p. 30.

¹¹³ *Ibid.*

¹¹⁴ *Ibid.*

¹¹⁵ N.MARTIAL-BRAZ, « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p.253

composante décisionnelle du droit à l'autodétermination de l'individu pour seulement la réduire à sa composante informationnelle. La protection se retrouve donc amputée d'une partie de ses caractéristiques ce qui risque de ne protéger que partiellement le salarié « homo numericus » de l'impact du progrès numérique et technologique sur sa vie privée et personnelle.

Toutefois, si le droit à la protection des données personnelles montre un attachement particulier au droit au respect de la vie privée du salarié, il s'avère que d'autres droits et libertés fondamentaux peuvent être atteints dans leur substance par les dispositifs de traitements des données personnelles des salariés.

Section 2 – La non-réductibilité de la protection des données à la protection de la vie privée

Face aux développements accrus des technologies, le droit à la protection des données personnelles permet, d'une part, de garantir au citoyen-salarié le respect de sa dignité (A) et d'autre part, de constituer un rempart aux pouvoirs décisionnels de l'employeur (B).

§1. La protection des données personnelles comme garante de la dignité des salariés

La dignité est inhérente à l'espèce humaine. Ne pas traiter l'Homme avec dignité revient donc à nier son appartenance à l'humanité¹¹⁶.

Le lien entre protection des données personnelles des salariés et dignité ne figure qu'au sein du recueil des directives pratiques du Bureau International du travail (BIT) relatif à la protection des données personnelles des travailleurs. Instrument de « droit mou » ce recueil fait néanmoins de la dignité un objectif global du droit à la protection des données personnelles¹¹⁷.

¹¹⁶ P.ADAM, « La dignité du salarié », *Rev. trav.* 2014, p.244.

¹¹⁷ BUREAU INTERNATIONAL DU TRAVAIL, Protection des données personnelles des travailleurs, Recueil de directives pratiques du BIT, Organisation internationale du travail, 1997, 52 p, art 1 valant préambule : « Les employeurs collectent des données personnelles sur les candidats à un emploi et sur les travailleurs à des fins diverses : être en conformité avec la législation; faciliter la sélection à l'embauche, la formation et la promotion; assurer la sécurité des personnes, le contrôle de la qualité, le service à la clientèle et la protection des biens de l'entreprise. Différentes lois nationales et normes internationales assujettissent le traitement des données personnelles à des règles contraignantes. L'emploi de techniques telles que la recherche documentaire informatisée, l'automatisation des systèmes d'information sur le personnel, la surveillance électronique, le dépistage génétique et les contrôles antidrogue rend nécessaire d'élaborer des dispositions sur la protection des données personnelles qui s'appliquent en particulier à l'utilisation des données personnelles des travailleurs, afin de préserver leur dignité, de protéger leur vie privée et de garantir leur droit fondamental de décider qui peut utiliser quelles données, à quelles fins et dans quelles conditions. »

Puisque les dispositifs de traitement des données personnelles ont augmenté les risques d'atteinte à la dignité des salariés, assurer la protection des données personnelles permet d'éviter les risques de discrimination (A) et d'objectivation du salarié (B).

A. La garantie contre la discrimination

Les discriminations portent atteinte à la dignité des salariés puisqu'elles portent atteinte à l'égalité de droit et de jouissance de droit en raison de la seule caractéristique d'un individu¹¹⁸. En droit du travail, le principe de non-discrimination est posé par l'article L.1132-1 du Code du travail. Si cet article a fait l'objet de nombreuses modifications, il est désormais interdit pour l'employeur de tenir compte de vingt-quatre motifs pour prendre une décision¹¹⁹. Ce principe irrigue toutes les phases de la relation contractuelle que ce soit lors de la conclusion du contrat de travail, de son exécution ou de sa rupture. L'employeur doit être objectif et ne pas prendre en compte un élément subjectif discriminant pour forger n'importe quelle décision. La prohibition apparaît alors « comme la traduction juridique d'une conception de l'Homme appréhendé en lui-même et pour lui-même »¹²⁰.

Or, les NTIC ont accentué les risques de discriminations puisqu'elles facilitent « la constitution de profils et la diffusion d'informations personnelles »¹²¹.

En matière de protection des données personnelles, le principe de non-discrimination est majoritairement concentré dans la notion de données dites sensibles. En effet, contrairement au BIT¹²², les textes législatifs dotés d'une véritable force contraignante ne font référence au

¹¹⁸ Déclaration Universelle des droits de l'Homme du 10 décembre 1948, préambule et article 1 et 2.

¹¹⁹ Article L.1132-1 du Code du travail, modifié par Loi n°2019-486 du 22 mai 2019 – art 190. Il est interdit de prendre en compte « l'origine du salarié, son sexe, ses mœurs, son orientation sexuelle, son identité de genre, son âge, sa situation de famille ou sa grossesse, ses caractéristiques génétiques, la particulière vulnérabilité résultant de sa situation économique, apparente ou connue de son auteur, son appartenance ou de sa non-appartenance, vraie ou supposée, à une ethnie, une nation ou une prétendue race, ses opinions politiques, ses activités syndicales ou mutualistes, ses convictions religieuses, son apparence physique, son nom de famille, son lieu de résidence ou sa domiciliation bancaire, ou en raison de son état de santé, de sa perte d'autonomie ou de son handicap, de sa capacité à s'exprimer dans une langue autre que le français ».

¹²⁰ Rapport annuel 2008 de la Cour de cassation, troisième partie : « Etude : les discriminations en droit social, les discriminations dans le travail » : « La prohibition des discriminations apparaît comme la traduction juridique d'une conception de l'homme appréhendé en lui-même et pour lui-même. Les règles d'égalité, en revanche, se rattachent à une conception des rapports sociaux entre les individus ou les groupes. La prohibition des discriminations est donc avant tout le résultat d'une pensée ontologique, tandis que les règles d'égalité sont le résultat d'une pensée sociologique. Les dispositions prohibant les discriminations n'interdisent pas que des différenciations soient opérées entre des personnes placées dans des situations identiques ou analogues. Elles empêchent seulement que ces différences soient fondées sur des critères précisément énumérés. Ainsi, l'article L. 1132-1 du code du travail donne une liste limitative des éléments dont la prise en considération est interdite ».

¹²¹ G.DESGENS-PASANAU, *op. cit.*, p.30.

¹²² Bureau International du Travail, Protection des données personnelles des travailleurs, Recueil de directives pratiques du BIT, Organisation internationale du travail, 1997, p. 4, article 5.10: «Le traitement des données personnelles ne devrait pas entraîner une discrimination illégale dans l'emploi ou la profession ». Voir également,

principe de non-discrimination qu'en énumérant les données dites sensibles dont le traitement est par principe interdit. Il en principe « 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, des données génétiques, des données biométriques ou des données relatives à leur santé ou à leur vie sexuelle ou à l'orientation sexuelle d'une personnes physiques »¹²³. Cet article prohibe donc les discriminations directes et indirectes¹²⁴.

Les données biométriques sont donc expressément considérées comme données dites sensibles, ce qui faisait défaut à la loi originelle. Ces données permettent de contrôler l'accès aux locaux ou services de l'entreprise¹²⁵. Elles sont définies comme résultant d'un « dispositif de traitement technique spécifique permettant d'identifier une personne à partir d'une ou plusieurs de ses caractéristiques biologiques ou comportementales, comme par exemple son empreinte digitale, le contour d'une main, l'iris d'un œil, son ADN ou bien encore son réseau veineux »¹²⁶. Chaque citoyen-salarié dispose en effet de caractéristiques biologiques qui lui sont propres et qui permettent de l'identifier de façon plus ou moins certaine selon la technique utilisée.

En intégrant cette donnée dans la catégorie de données dites sensibles (donc en principe interdite de collecte), le législateur a souhaité renforcer la protection des citoyens-salariés à l'égard des traitements de leurs données.

Le lien étant défini, il convient de s'interroger sur les répercussions que peuvent éventuellement avoir le traitement des données sensibles sur les droits fondamentaux des salariés, notamment lorsqu'elles portent sur des éléments matériels « traçables » et inhérent à chaque individu comme les empreintes digitales. C'est la dignité même du salarié qui est

et de manière plus précise, p. 6, dans son article 6.5 relatif à l'interdiction pour l'employeur de collecter des données concernant la « vie sexuelle des travailleurs », les « opinions politiques, religieuses ou autres des travailleurs » et les « condamnations pénales des travailleurs ». Le BIT propose également de réserver le même sort aux « données personnelles concernant l'appartenance ou l'activité syndicale d'un travailleur » dans l'article 6.6 et aux données médicales dans l'article suivant, sous réserve du respect d'obligations légales

¹²³ Règl, n°(UE) 2016/679, op., cit., art 9.1 ; Loin°78-17,6 janv 1978, art 8, I mod par L.2018-493, 20 juin 2018.

¹²⁴ Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations, art 1 al. 1 : « Constitue une discrimination directe la situation dans laquelle, sur le fondement d'un des principes prohibés, une personne est traitée de manière moins favorable qu'une autre ne l'est, ne l'a été ou ne l'aura été dans une situation comparable. Art 1 al. 2 : « Constitue une discrimination indirecte une disposition, un critère ou une pratique neutre en apparence, mais susceptible d'entraîner, pour l'un des motifs mentionnés au premier alinéa, un désavantage particulier pour des personnes par rapport à d'autres personnes, à moins que cette disposition, ce critère ou cette pratique ne soit objectivement justifié par un but légitime et que les moyens pour réaliser ce but ne soient nécessaires et appropriés ».

¹²⁵ Loi n°2018-493, 20 juin 2018 : JO, 21 juin, art. 8, II, 9°, nouveau.

¹²⁶ L.GAMET, « Biométrie et travail », *Dr.soc* 2019, p. 422.

susceptible d'atteinte lors d'une éventuelle l'utilisation par les entreprises de ces données dans la mesure où elles sont susceptibles de lui nuire.

En effet, à l'heure où le fichage et le profilage sont en vogue, ces citoyens-salariés pourraient être fichés selon leur origine, santé voire leur orientation sexuelle. Le professeur François Rigaux considère que la notion de profil « présente une analogie étroite avec le racisme »¹²⁷. En effet, le profilage consiste à « imputer à un individu certains faits de comportement qui seraient communs au groupe auquel il est censé appartenir et distinguerait les membres du groupe à l'intérieur de la population globale »¹²⁸. Il y aurait donc atteinte à la dignité en faisant utilisation de ce fichier pour choisir un candidat à un emploi, pour décider de surveiller seulement certains individus en fonction de leur ethnie voire d'empêcher l'accès à une promotion en raison d'un problème de santé d'un salarié puisque « les technologies de construction d'individus statistiques » permettent « l'établissement de profils individuels »¹²⁹. Ici, l'intimité du salarié est donc touchée mais également sa dignité et son droit à ne pas être discriminé tel que réprimé par l'article L.1132-1 du Code du travail.

De même, l'utilisation de dispositifs de contrôle d'accès biométrique interroge sur les enjeux en termes de sécurité et d'usurpation d'identité preuve en est que les hackers usurpent aisément l'identité d'un individu en trompant les lecteurs d'empreintes digitales. En effet, face à l'augmentation des scandales liés à des failles de sécurité, il est possible de s'interroger sur la pertinence de ces dispositifs puisque, comme l'a souligné Guillaume Desgens-Pasanau, « s'il est possible de faire opposition à sa carte bancaire quand on se l'est faite dérober, qu'en est-il en revanche si c'est le gabarit de son empreinte digitale que l'on s'est fait dérober? »¹³⁰.

En définitive, c'est par l'interdiction de principe du traitement de données sensibles que le principe de non-discrimination est consacré. Si la loi paraît plus complète, il est en revanche regrettable que le législateur n'ait pas indiqué explicitement que cette interdiction a pour but de protéger le principe de non-discrimination, même si une comparaison entre le type des données sensibles avec la liste des motifs discriminatoires permet d'enlever le doute tant il recouvre presque exactement le champ couvert par ces motifs.

¹²⁷ F.RIGAUX, « La protection de la vie privée et les autres biens de la personnalité », *Bruylant LGDJ*, 1990.

¹²⁸ *Ibid.*

¹²⁹ N. OCHOA, *op.,cit.*,p.476.

¹³⁰ G. DESGENS-PASANAU, *op., cit.*,p.195.

Ainsi, en assurant une protection des données personnelles des salariés, le risque d'atteinte à la dignité du salarié est minoré. Cependant le développement technologique n'a pas eu seulement pour conséquence d'augmenter le risque de discrimination mais a également augmenté le risque de transformer le salarié en une chose, lui faisant perdre tout degré de subjectivité et le réduisant ainsi à un animal d'élevage dont la seule finalité est la productivité.

B. La garantie contre l'objectivation

Si le lien entre protection des données personnelles et objectivation du salarié n'apparaît pas d'emblée évident, la doctrine considère qu'assurer sa protection permet de lutter « contre les entreprises de la donnée tendant à la réification du salarié » c'est-à-dire son objectivation¹³¹.

Dans les relations de travail, l'objectivation correspond à la réduction du salarié à un objet. Or cette réduction a un impact sur les relations de travail, notamment en termes de santé et de qualité de vie au travail, mais aussi en termes de productivité puisqu'assimilé à un objet, le salarié perd tout intérêt dans le résultat de son travail et perd ainsi en productivité¹³².

Il ne faut pas oublier qu'un des fondements déterminant de la Société est la distinction entre la personne humaine et la chose puisqu'elle a permis de libérer l'Homme de l'esclavage¹³³. Cependant le progrès numérique et technologique a tendance à réduire le salarié à son utilité, à l'instar d'un simple moyen de productivité.¹³⁴ Mais considérer le salarié comme un objet revient à nier son appartenance à la qualité du genre humain. Le salarié ne doit donc en aucun cas être instrumentalisé sur le modèle d'une chose, sous peine de porter atteinte à sa dignité¹³⁵.

¹³¹ N. OCHOA, op.,cit., p.482.

¹³² A. SUPIOT, « Fragments d'une politique législative du travail », *Dr.soc.*, p.1151 : « À ce modèle physique de l'horloge, qui dès le XVIII^{ème} siècle conduisait à voir dans l'homme lui-même une machine, s'est ajouté au XIX^{ème} siècle le modèle biologique de la sélection naturelle, qui a conduit au darwinisme social et continue de sévir sous les espèces de l'ultralibéralisme et de la compétition de tous contre tous. À ces représentations, qui ne s'annulent pas mais se superposent, s'ajoute aujourd'hui celle de l'homme programmable, portée par la cybernétique et la révolution numérique. Son objet fétiche n'est plus l'horloge et son jeu de forces et d'engrenages, mais l'ordinateur et son traitement numérique des signaux. L'ordinateur obéit à des programmes plutôt qu'à des lois. Autorisant une extériorisation de certaines facultés cérébrales de l'être humain, il ouvre une ère nouvelle dans notre rapport aux machines, aussi bien que dans le contenu et l'organisation de notre travail »

¹³³ C.WILLMANN, « Esclavage – Travail forcé – Traite des êtres humains », *Répertoire de droit pénal et de procédure pénale*, octobre 2006 (actualisation : janvier 2017) : « La soumission d'un salarié à des conditions de travail indignes doit être assimilée à une pratique esclavagiste, lorsqu'elle tend à faire considérer le travailleur comme un prolongement d'une machine-outil (Cass.crim. 4 mars 2003, n° 02-82194).

¹³⁴ G. LOISEAU, « Typologie des choses hors du commerce », *RTD civ.*, 2000, p. 46.

¹³⁵ G. LOISEAU, « Des droits patrimoniaux de la personnalité en droit français », *Rev. dr. McGill*, juin 1997, p. 319 et s.

Cette crainte n'est pas nouvelle et est bien antérieure au développement de l'informatique. En effet Karl Marx considérait que c'est par le travail que l'être humain s'affirme. En étant l'essence de l'Homme, le travail fait de lui ce qu'il est. Toutefois, dans le système capitaliste, le travail ne permet plus à l'ouvrier d'affirmer son existence. Karl Marx avait conscience que le problème était la forme qu'avait pris le travail. D'après lui, cette nouvelle forme de travail anéantirait le sujet du travailleur puisque les produits du travail sont séparés de son sujet producteur (en l'occurrence les travailleurs). En étant séparé de l'objet de son travail, le travailleur peut donc aussi devenir un objet : c'est le phénomène de chosification¹³⁶.

Précurseur, Karl Marx avait vu juste. Le progrès technologique a modifié davantage la forme de travail en ayant tendance à administrer les salariés comme des choses. L'accroissement technique comme technologique altère le rapport de l'homme à la machine : l'histoire de l'humanité est celle d'une progression de la pénétration de l'un dans l'autre. Le professeur Alain Supiot rend compte de ce phénomène, parachevé par le numérique¹³⁷.

Tout d'abord, « la révolution numérique présente effectivement un risque de réduction de l'ipsité » à la « mêmeté »¹³⁸ car le salarié est réduit à un ensemble de données factuelles. L'exemple des dispositifs biométriques est pertinent. Avec ces dispositifs, le salarié se trouve réduit à un de ses éléments physiques et la généralisation de la biométrie risque d'aboutir à « la réduction de la personnalité à l'humanité biologique »¹³⁹. Pour la Commission nationale consultative des droits de l'homme (CNCDH), « la collecte de ces éléments représentatifs de l'être touche la dignité humaine en ce qu'elle réduit chacun à l'extraction de son patrimoine biologique »¹⁴⁰. Grâce à cette technique, l'obtention de l'identification d'une personne peut se faire à son insu sur la base de traces physiques.

La protection des données personnelles permet aussi d'éviter les méfaits que peuvent engendrer des décisions prises à l'encontre des individus par des objets tels que les programmes algorithmiques ou les robots¹⁴¹. L'objectivation du salarié est telle qu'elle rend parfois

¹³⁶ K.MARX, « Manuscrits de 1844 », Flammarion, 2006, p.156.

¹³⁷ A.SUPIOT, « La Gouvernance par les nombres », Cours au Collège de France 2012-2013.

¹³⁸ N.OCHOA, *op.,cit.*, p : 482

¹³⁹ N.OCHOA, *op.,cit.*, p.482.

¹⁴⁰ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *art., préc.*

¹⁴¹ L'exemple du nouveau système d'Admission Post-Bac dont la fonction est de recueillir les souhaits d'orientation des bacheliers et d'attribuer les places dans l'enseignement supérieur en fonction de divers facteurs comme l'académie du siège de l'établissement et du rang de classement du vœux, s'est avéré vivement critiqué

indiscernable son remplacement par ces derniers. Cette hybridation diminue le rôle de l'humain et sa part de subjectivité dans le processus productif et laisse plus de place à la machine qui gagne en autonomie. A titre d'exemple, la « machine learning » (apprentissage automatique) et le « deep learning » (apprentissage en profondeur) permettent d'étayer ces propos. Le premier permet aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet. Le salarié entraîne le système en lui fournissant un nombre impressionnant de données à partir desquelles la machine établira elle-même les opérations à effectuer pour accomplir la tâche. L'écriture prédictive des emails en constitue un exemple concret. Le deep learning va encore plus loin puisqu'il parcourt un certain nombre d'exemples identifiés comme semblables pour en déterminer des caractéristiques communes utiles pour la reconnaissance. Il pourra s'agir des dispositifs de reconnaissances faciales par exemple¹⁴².

Ainsi, afin d'éviter d'annihiler l'humain dans le processus décisionnel, l'article 22 du RGPD prévoit que « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »¹⁴³. Le profilage est fréquemment utilisé pour notamment permettre à un employeur de déterminer les performances de ses salariés au travail. Or il est possible que des décisions soient prises par le biais d'algorithmes appliquées aux données personnelles des salariés sans qu'aucun être humain n'intervienne dans le processus. En permettant au salarié de demander l'intervention d'une personne humaine pour réexaminer la situation, la protection des données personnelles permet d'éviter la généralisation d'une forme d'hybridation entre l'humain et la machine¹⁴⁴.

La protection des données personnelles joue alors « le rôle de réserve de subjectivité face à une évolution du numérique qui tend au moins pour partie à l'objectivation »¹⁴⁵ du salarié¹⁴⁶.

puisque les bacheliers font désormais face à un algorithme pour déterminer la suite de leurs études. Les ratés ne sont pas en manque : absence d'attributions de place quelques jours avant la rentrée, mauvaise attribution, etc.

¹⁴² Rapport CNIL, déc 2017, « comment permettre à l'homme de garder la main ? – Les enjeux éthiques des algorithmes et de l'intelligence artificielle ».

¹⁴³ Règl. n° (UE) 2016/679 du Parlement européen et du Conseil, 27 avr.2016, art 22.

¹⁴⁴ Cependant cette affirmation est à nuancer si « la mobilisation d'algorithmes auto-apprenants est certes évitée, expliquer la motivation de la décision algorithmique, reposant sur des corrélations de données de plus en plus complexes et non plus sur la logique causale qui la caractérise traditionnellement, est un défi et l'intervention humaine prévue en amont et en aval de la décision ne soit que factice ». V. L.CLUZEL-METAYER Et E.DEBEAETS, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA 2018*. p.1101.

¹⁴⁵ N.OCHOA, *op.cit.*, p.482.

¹⁴⁶ A.SUPIOT, « Le travail est-il encore un droit ? », Les Cours du Collège de France, La Grande Table des Idées, France Culture, 27 mars 2019.

En définitive, la protection des données personnelles permet de préserver le salarié d'atteinte à sa dignité, que ce soit en le protégeant contre les discriminations ou contre sa réification. Toutefois, l'enjeu de la protection n'est pas seulement de garantir la dignité du salarié mais également de protéger le salarié des excès de son employeur et ainsi d'être un rempart au pouvoir de ce dernier.

§2.La protection des données personnelles comme rempart au pouvoir de l'employeur

Le droit à la protection des données personnelles permet de protéger le salarié à l'égard des empiètements arbitraires de l'employeur (A) mais également de préserver ce dernier d'une certaine opacité de l'entreprise (B).

A. La garantie contre l'arbitraire de l'employeur

L'adjectif arbitraire est souvent employé pour désigner « ce qui dépend de la seule volonté, ce qui n'est pas lié par l'observation de règle »¹⁴⁷ Appliquée aux relations de travail, la notion d'arbitraire renvoie au caractère d'une décision prise par l'employeur selon son bon vouloir et qui n'est donc pas le résultat de l'application d'une règle juridique. Le progrès numérique et technologique a accentué le pouvoir arbitraire de l'employeur et la « peur d'atteintes aux libertés publiques par la rupture de l'équilibre entre gouvernants et gouvernés, la multiplications des informations à la disposition des gouvernants leur conférant un pouvoir accru sur les gouvernés »¹⁴⁸. Ce progrès a alors amplifié le besoin d'encadrement puisqu'il « constitue en lui-même un facteur de concentration des pouvoirs »¹⁴⁹. La prolifération massive des NTIC dans l'entreprise a accentué le risque de déséquilibre entre les détenteurs d'informations (les entreprises) et les individus concernés (salariés).

Face à ce risque d'arbitraire, le droit du travail et les mécanismes de protection des données personnelles des salariés se sont efforcés de comporter, en leur sein, des garanties propres à juguler le surcroît d'arbitraire suscité par l'apparition et le développement des NTIC, en matière d'exercice du pouvoir de direction et de sanction de l'employeur. Si la France n'a

¹⁴⁷ Le nouveau Petit Robert, dictionnaire alphabétique et analogique de la langue française, Le Robert, 2010.

¹⁴⁸ J. FRAYSSINET ET P.KAYSER, « La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret du 17 juillet 1978 », *RDP*, 1979, p. 632.

¹⁴⁹ A. VITALIS, « Pouvoir et Libertés », Paris, *Economica*, 1981, p.113.

pas formalisé, dans le droit à la protection des données, une garantie contre l'arbitraire, il en est autrement de nos pays voisins comme l'Espagne avec la notion d'« habeas corpus »¹⁵⁰.

Malgré cette absence de formalisation, il s'avère que des garanties procédurales sont prévues. En informant les salariés et la collectivité de travail de l'existence des dispositifs de traitements des données et leurs finalités, le droit veille à mettre en place tout un ensemble de dispositifs évitant les prises de décisions subjectives de l'employeur.

En effet, les NTIC permettent de prendre facilement une décision ayant des effets juridiques sur la base des données personnelles des salariés. Ainsi des garanties procédurales doivent être mises en place pour respecter les droits de la défense du salarié afin de lui éviter qu'une décision arbitraire ne soit fondée sur le traitement desdites données.

En mettant en place un corpus juridique à respecter, l'objectif est d'apaiser les relations entre subordonnants et subordonnés en leur permettant de prévoir les conséquences de leurs actes. L'avènement de la « société de l'information » étant caractérisé par la multiplication exponentielle des traitements de données personnelles, l'obligation de prévisibilité s'affirme donc comme un rempart contre l'arbitraire.

Ainsi si la protection des données personnelles apparaît comme garante contre l'arbitraire de l'employeur, elle apparaît également comme une garantie contre les pratiques opaques des entreprises.

B. La garantie contre l'opacité de l'entreprise

C'est à travers les dispositifs d'alertes professionnelles que la transparence des entreprises vis-à-vis de leur gouvernance et pratique entrepreneuriales est garantie.

Initialement destinées à protéger les travailleurs face aux risques de discrimination et de harcèlement moral, la loi américaine « Sarbanes Oxley » (« SOX ») a donné aux lanceurs d'alerte un nouveau rôle en les faisant acteurs de la lutte contre la corruption et la fraude notamment fiscale et environnementale¹⁵¹.

¹⁵⁰ N.OCHOA, *op.cit.*, p.490. La notion d'habeas corpus est une notion juridique qui énonce une liberté fondamentale, celle de ne pas être emprisonné sans jugement, contraire de l'arbitraire qui permet d'arrêter n'importe qui sans raison valable. La notion d'« habeas data » est alors la notion d'« habeas corpus » appliquée à la société numérique. «El habeas data es una acción jurisdiccional propia del derecho, normalmente constitucional de cuarta generación, que confirma el derecho de cualquier persona física o jurídica para solicitar y obtener la información existente sobre su persona, y de solicitar su eliminación o corrección si fuera falsa o estuviera desactualizada».

¹⁵¹ Sarbanes-Oxley Act, 30 juill. 2002 : Public Law 107-204. - V. aussi le Dodd-Franck Act, 21 juill. 2010 : Public Law 111-203.

Si l'article 6 de la loi dite « Sapin II »¹⁵² a le mérite de donner une définition du lanceur d'alerte, cette loi va plus loin qu'une simple consécration de définition puisqu'elle instaure l'obligation, depuis le 1^{er} janvier 2018, de mettre en place, pour les entreprises d'au moins cinquante salariés, un dispositif de « recueil des signalements », ainsi que la désignation d'un référent chargé de recueillir les alertes¹⁵³.

Par dispositif d'alerte professionnelle (ou « whistleblowing »), il convient d'entendre tout dispositif mis à la disposition des salariés, comme par exemple un numéro de téléphone « ligne éthique » ou une adresse électronique spécifique, leur permettant de signaler des problèmes pouvant sérieusement affecter l'activité d'une entreprise ou engager gravement sa responsabilité¹⁵⁴.

La mise en œuvre de ces dispositifs fait notamment suite à l'adoption de la loi « SOX » qui impose la mise en place de tels dispositifs pour les sociétés cotées en bourse et leurs filiales étrangères, et ce afin notamment de prévenir l'éventualité de fraudes financières ou comptables au sein des entreprises¹⁵⁵. La France a donc dû suivre cette réglementation même si au début la CNIL s'est montrée réticente¹⁵⁶.

Si le progrès numérique, et avec lui les NTIC, a permis la mise en place de ce dispositif informatisé en permettant de lutter contre l'impunité des entreprises et l'omerta qui pèse sur leurs pratiques, il fait l'objet d'une haute surveillance tant les risques en matière de protection des personnes à l'égard des traitements de leurs données sont nombreux. En effet, ce dispositif engendre la collecte et le traitement de nombreuses données personnelles que ce soit l'identité de l'auteur de l'alerte, les personnes mises en cause et les faits relatés pouvant toucher aux infractions de droit pénal.

¹⁵² Loi dite « Sapin II » n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, JORF n°0287 du 10 décembre 2016, art 6 : « une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance ».

¹⁵³ Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte, JORF n°0093 du 20 avril 2017, applicable depuis le 1er janvier 2018.

¹⁵⁴ Loi dite « Sapin II » n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, JORF n°0287 du 10 décembre 2016, art 16.

¹⁵⁵ F.BARRIERE, « Les dispositifs d'alertes professionnelles : le temps de l'apaisement ? », *Rev. sociétés* 2011, p.276

¹⁵⁶ Concernant le projet « hotline » de chez McDonald's France, la CNIL avait refusé à cette enseigne l'utilisation de ce mécanisme d'alerte professionnelle puisqu'elle craignait que ces dispositifs conduisent à un « système organisé de délation professionnelle », et engendrent « des risques de dénonciations calomnieuses et de stigmatisations des employés objet d'une alerte éthique. V. CNIL, délib., n° 2005-110 et n° 2005-111, 26 mai 2005.

Par conséquent, vu l'impact de ces dispositifs sur la protection des données personnelles, les législations qui se sont succédées ont tenté d'assurer, durant tout le cycle de vie de l'alerte, une protection sérieuse des données personnelles collectées par ces dispositifs. Si les déclarations simplifiées adoptées dans le passé par la CNIL n'ont plus à être utilisées, elles constituent toujours des référentiels utiles pour analyser le niveau de conformité du traitement mis en œuvre¹⁵⁷.

Tout d'abord, sauf exceptions¹⁵⁸, l'identité de l'auteur de l'alerte est confidentielle¹⁵⁹. En effet, son identité doit être tenue secrète. Il est regrettable qu'en France la législation ne protège pas les lanceurs d'alerte par l'anonymat, contrairement au Royaume-Unis. Leur identité ne peut pas être divulguée, sauf à l'autorité judiciaire et sauf s'ils y consentent¹⁶⁰. Si l'anonymat peut être vu comme un moyen de rassurer l'auteur de l'alerte sur les éventuelles conséquences de sa dénonciation, et ainsi rendre le dispositif efficace, la CNIL considère qu'au contraire il augmente les risques de mises en cause abusives ou disproportionnées, facilite la protection du salarié contre d'éventuelles représailles et permet un meilleur traitement de l'alerte en ouvrant la possibilité de demander à son auteur des précisions complémentaires¹⁶¹.

De même le lanceur d'alerte bénéficie, en plus d'une immunité pénale, d'un réel statut protecteur puisqu'il ne peut faire l'objet de rétorsions de la part de son employeur sous peine d'annulation de la décision et de réparation¹⁶², et ne peut pas être sanctionné en cas de défaut d'activation du dispositif puisque ce dernier est facultatif¹⁶³.

Ensuite, l'identité de la personne mise en cause doit également être protégée. Les éléments permettant de l'identifier ne peuvent pas être divulgués, sauf à l'autorité judiciaire, et que si le bien-fondé de l'alerte a pu être préalablement établi.

¹⁵⁷ V.AU-004 portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre des dispositifs d'alerte professionnelle.

¹⁵⁸ CNIL, délib., n° 2017-191., 22 juin 2017 : « Par exception, l'alerte d'une personne qui souhaite rester anonyme peut être traitée sous les conditions suivantes : la gravité des faits mentionnés est établie et les éléments factuels sont suffisamment détaillés ; le traitement de cette alerte doit s'entourer de précautions particulières, telles qu'un examen préalable, par son premier destinataire, de l'opportunité de sa diffusion dans le cadre du dispositif. »

¹⁵⁹ CNIL, délib. n° 2017-095., 23 mars 2017.

¹⁶⁰ CNIL, délib. n° 2018-042., 8 février 2018.

¹⁶¹ *Ibid.*

¹⁶² Article L.1132-3-3 du Code du travail ; L.1134-1 du Code du travail ; Cass.soc., 30 juin 2016, n°15-10.557 : « Le fait pour un salarié de porter à la connaissance du procureur de la République des faits concernant l'entreprise qui lui paraissent anormaux, qu'ils soient ou non susceptibles de qualification pénale, ne constitue pas en soi une faute; en raison de l'atteinte qu'il porte à la liberté d'expression, en particulier au droit pour les salariés de signaler les conduites ou actes illicites constatés par eux sur leur lieu de travail, le licenciement d'un salarié prononcé pour avoir relaté ou témoigné, de bonne foi, de faits dont il a eu connaissance dans l'exercice de ses fonctions et qui, s'ils étaient établis, seraient de nature à caractériser des infractions pénales, est frappé de nullité »

¹⁶³ G.DESGENS-PASANAU, *op., cit.*, p.206.

Enfin, la gestion des risques informatiques doit être rigoureuse puisque ces dispositifs sont sujets à de nombreuses cyberattaques destinées à récupérer les données qui y sont inscrites ou alors à bloquer complètement le réseau pour mettre en péril l'alerte qui devait être lancée. Ainsi, afin de prévenir tout détournement ou utilisation frauduleuse des données recueillies lors du signalement, le dispositif d'alerte doit répondre aux exigences du RGPD en matière de sécurité.

En définitive, les dispositifs d'alerte font l'objet d'un encadrement juridique afin de protéger à la fois la personne auteure de l'alerte ainsi que les données qui figureront dans le dispositif. Cette protection est utile afin de prévenir les abus dans l'utilisation de ce dispositif, initialement destiné à favoriser la paix sociale. Il serait regrettable qu'ils produisent l'effet inverse en la remettant en cause¹⁶⁴.

CONCLUSION DU CHAPITRE I

La multiplication et la démocratisation des dispositifs de traitements de données personnelles au sein de l'entreprise interrogent le sort de la protection des données personnelles des salariés.

Citoyens à part entière, les salariés bénéficient de la protection de leur vie privée dans l'enceinte de l'entreprise. Appliquée à la relation de travail, cette notion de vie privée entendue comme le cercle intime de l'individu s'étend et prend en compte de façon plus générale, le cercle personnel du salarié.

L'avènement de l'Homo numericus induit par la Révolution numérique a transformé la notion de vie privée pour y inclure la liberté dans la vie privée. Face au progrès numérique et technologie, assurer une protection des données personnelles permet de garantir le droit à l'autodétermination décisionnelle et informationnelle du salarié.

Toutefois, il ne faut pas réduire l'enjeu de protection des données personnelles au seul droit au respect de la vie privée quand bien ce droit deviendrait démesure. L'enjeu de la protection est plus noble et plus grand puisqu'il vise à sauvegarder tous les droits et libertés

¹⁶⁴ N.LENOIR ; A.DILL ET H.BERION, « Lanceurs d'alerte - Alerte professionnelle et protection des données personnelles », *La Semaine Juridique Edition Générale* n° 19-20, 7 Mai 2018, doct. 553.

fondamentaux du salarié. En effet, si le droit au respect de la vie privée permet de protéger le salarié contre les modalités techniques d'atteinte, la protection des données personnelles vise à préserver le salarié des atteintes susceptibles d'être opérées par la voie informatique et technologique. Parmi ces risques, on retrouve les risques d'atteinte à la dignité des salariés.

Dès lors, la protection des données personnelles permet, d'une part d'éviter les risques de discrimination, et d'autre part, les risques d'objectivation du salarié, réduit à sa seule fonction d'élément productif.

Enfin, l'enjeu est également de préserver le salarié de tout arbitraire et permet d'instaurer une transparence sur les pratiques des entreprises, indispensable au climat de paix social récemment malmené.

Au regard de ce formidable enjeu qu'est la protection des données personnelles des salariés, il convient de retracer les moyens permettant d'assurer sa protection.

Chapitre II : LES MOYENS DE LA PROTECTION

Cette question des moyens de la protection est déterminante :

D'une part, car elle nécessite d'examiner avec précision les garanties mises en place destinées à éviter toute forme d'atteinte à la protection des données personnelles des salariés dont l'examen de la licéité des traitements constitue le centre de gravité de ladite protection (Section 1).

D'autre part, car elle implique d'examiner les moyens mis en œuvre afin de rendre effective la protection des données personnelles des salariés (Section 2).

Section 1 – L'examen de la licéité

La disponibilité des données personnelles des salariés est conditionnée par l'existence de principes liés à la collecte (§1) et au traitement desdites données (§2) tenant à leur licéité.

§1. La licéité par l'existence de principes liés à la collecte des données

Pour qu'il puisse y avoir traitement de données personnelles, encore faut-il qu'il y ait collecte de données personnelles. Or pour qu'une donnée puisse être traitée, sa collecte doit juridiquement être permise. Ainsi, pour que les droits et libertés fondamentaux des salariés puissent être préservés, il est apparu nécessaire d'encadrer la collecte tant au regard de la nature des données collectées (A) que de leur qualité (B).

A. L'importance de la nature des données collectées

Toutes les données personnelles ne sont pas susceptibles de collectes. Le droit intervient ici pour interdire la collecte de certaines catégories de données. Appliquées aux relations de travail, les données personnelles des salariés susceptibles d'intéresser l'employeur doivent être objectives, c'est-à-dire en rapport avec l'activité professionnelle de ces derniers.

Les données se rattachant à la personnalité du salarié sans rapport avec ses compétences professionnelles sont donc, en principe proscrites. Sont concernées les données dites sensibles¹⁶⁵. La nature des données conditionne alors la licéité du traitement.

¹⁶⁵ Règl. n° (UE) 2016/679, *op. cit.*, art 9. Il est par principe interdit de collecter les données personnelles se rapportant à la subjectivité des salariés c'est-à-dire celle qui font apparaître « l'origine raciale ou ethnique, les

Toutefois, comme toute interdiction de principe, des exceptions limitativement énumérées sont à relever. Si la loi française prévoyait un certain nombre d'exceptions, le RGPD a élargi la liste ce qui permet aux employeurs de collecter ces données sous certaines conditions. Parmi les conditions, relatives aux relations de travail, le traitement doit être nécessaire « aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable de traitement ou de la personne concernée ». De même, le traitement sera autorisé « s'il est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale (...) ». Par conséquent, les données relatives à la santé des salariés comme les arrêts de travail sont autorisées puisque nécessaires, d'une part à l'entreprise pour la gestion de ses ressources humaines, et d'autre part, pour le salarié pour l'octroi des indemnités journalières et de la prise en compte de son délai de carence.

Concernant les données biométriques, la loi du 20 juin 2018 a maintenu une dérogation à l'interdiction¹⁶⁶. S'il n'y a plus d'autorisation à obtenir auprès de la CNIL¹⁶⁷, cette dernière a toutefois élaboré un règlement type servant de référentiel à l'employeur, pour assurer la conformité des dispositifs de traitement ayant pour finalité « le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail »¹⁶⁸.

Ces données ne sont pas les seules concernées. Sont exclues les données relatives aux condamnations pénales et aux infractions ou mesures de sûreté¹⁶⁹. Les entreprises ne sont donc pas autorisées à collecter les données relatives aux qualifications et condamnations pénales puisque l'obtention des casiers judiciaires et la constitution de casiers judiciaires privés sont interdites¹⁷⁰.

Enfin, une autre donnée est sujette à polémique même si d'apparence elle peut paraître anodine. Il s'agit du numéro de sécurité sociale (NIR). Ce numéro est composé d'une chaîne

opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle » du salarié.

¹⁶⁶ Règl, n°(UE) 2016/679, *op., cit.*, art 9.1 ; Loi n°78-17,6 janv 1978, art 8, I mod par L.2018-493, *op., cit.*

¹⁶⁷ Autorisation Unique (AU) 052 sur les dispositifs biométriques permettant aux personnes de garder la maîtrise de leur gabarit biométrique et AU-053 sur les dispositifs biométriques ne garantissant pas cette maîtrise.

¹⁶⁸ CNIL, délib n°2019-001 du 10 janvier 2019.

¹⁶⁹ Règl. n° (UE) 2016/679, *op., cit.*, art 10.

¹⁷⁰ N.METALLINOS, « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Daloz IP.IT*, 2016, p.588.

de caractères permettant de déterminer le sexe, le mois et l'année de naissance et, dans la majorité des cas, le lieu de naissance. Il est unique et pérenne dans la mesure où un seul numéro est attribué à chaque individu dès sa naissance, et il est fiable puisque certifié par l'INSEE à partir des données d'état civil transmises par les mairies. Puisqu'il est particulièrement identifiant et signifiant, il « facilite les opérations de « chaînage » de données, d'interconnexion généralisée, voire d'utilisation détournée de fichiers puisqu'il rend plus aisées les possibilités de rapprochement des fichiers et, *in fine* le fichage généralisé des personnes »¹⁷¹.

Or, malgré la menace pour les droits et libertés fondamentaux des salariés, le RGPD est muet à son sujet contrairement à l'ancienne loi « Informatique et libertés » qui soumettait la mise en œuvre d'un traitement incluant le NIR à une autorisation préalable de la CNIL¹⁷². Sonnant le glas des formalités préalables, le décret du 19 avril 2019¹⁷³ est venu encadrer par voie réglementaire l'utilisation du NIR par les employeurs¹⁷⁴.

Ainsi dans le cadre de leurs activités, si les entreprises sont dans l'obligation d'utiliser le NIR, elles sont en revanche cantonnées à de strictes conditions afin d'éviter toutes réutilisations ultérieures illicites.

En définitive, ces données à risque mettent en avant un pan important de la personne du salarié. Comme par nature elles ne sont pas objectives mais seulement parfois nécessaires pour l'activité de l'entreprise, il est alors indispensable que ces données soient anonymisées ou cryptographiées afin de « supprimer tout caractère identifiant par des codes statistiques rendant impossible leur ré-identification »¹⁷⁵.

Ainsi, en interdisant ou en encadrant la collecte de certaines catégories de données, le droit veut assurer la protection des droits et libertés fondamentaux des salariés. D'autres conditions tenant à la qualité des données collectives viennent s'y greffer.

¹⁷¹ G.DESGENS-PASANAU, *op. cit.*, p. 85.

¹⁷² L.n°78-17,6 janv 1978, ancien art 25 ; CNIL, 29 nov. 1983 n°83-058, portant recommandation sur l'emploi du NIR admettant le recours au NIR pour les employeurs et les organismes de sécurité sociale uniquement dans le cadre de ces relations.

¹⁷³ Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire, JORF du 21 avril 2019.

¹⁷⁴ Ils n'y sont autorisés que pour remplir leurs obligations déclaratives notamment celles relatives à la « déclaration sociale nominative, pour le traitement automatisé de la paie et de la gestion du personnel résultant de dispositions légales ou réglementaires et de conventions collectives concernant les déclarations, les calculs de cotisations et de versement destinés aux organismes de sécurité sociale et de prévoyance ».

¹⁷⁵ A.LECOURT, « RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises », *Dalloz IP/IT*, 2019, p.205

B. L'importance de la qualité des données collectées

La qualité des données collectées est une condition nécessaire à la licéité du traitement dans la mesure où si certaines données sont en principe interdites de collecte, certaines étant exemptes de traitement.

Tout d'abord, la qualité de la donnée tient à la loyauté de sa collecte¹⁷⁶. Cette obligation de loyauté implique l'obligation pour l'employeur de collecter les données directement auprès du salarié concerné par le traitement. Toute collecte indirecte entraîne donc, par principe, l'illicéité du dispositif de traitement. Cependant, il est admis que la collecte de références auprès de l'environnement professionnel du candidat (employeurs, maître de stage, etc) soit permise dès lors qu'elle n'est pas faite à l'insu du candidat¹⁷⁷. Puisque la collecte indirecte est en principe proscrite, il n'est en revanche pas admis qu'un employeur puisse collecter les informations personnelles qu'un candidat aurait rendues publiques sur Internet et ce, même si ces informations l'intéressent¹⁷⁸. Ce n'est donc pas « parce qu'une information est librement accessible qu'elle est librement réutilisable »¹⁷⁹. Il n'est donc pas possible « d'aspirer les profils de millions de personnes sur les réseaux sociaux pour étoffer sa base de données »¹⁸⁰.

Ensuite, les données personnelles collectées ne peuvent l'être que pour « un usage déterminé, explicite et légitime et ne peuvent être traitées ultérieurement d'une manière incompatible avec ces finalités »¹⁸¹. La qualité de la donnée collectée tient ici au fait qu'elle doit obéir à une destination : un objectif préalablement défini et déterminé.

De même, elles doivent être non seulement « exactes mais aussi, si nécessaire, tenues à jour »¹⁸². L'inexactitude d'une donnée entraîne donc sa suppression ou sa rectification dans les plus brefs délais. L'installation de logiciels permettant de tracer ces modifications est donc conseillée.

¹⁷⁶ Règl. n° (UE) 2016/679, *op., cit.*, art. 5 – a : « Les données personnelles doivent être collectées de manière loyale ».

¹⁷⁷ G.DESGENS-PASANAU, *op., cit.*, p.5.

¹⁷⁸ *Ibid.*

¹⁷⁹ *Ibid.*

¹⁸⁰ CE., 12 mars 2014, n°353193. En l'espèce, le Conseil d'Etat a confirmé l'avertissement public prononcée par la CNIL envers la Société Pages Jaune Groupe pour avoir aspiré les profils issus de réseaux sociaux, ce qui constituait une collecte déloyale à l'égard des internautes concernés car ceux-ci n'en étaient pas informés au préalable.

¹⁸¹ Règl.n°(UE) 2016/679, *op., cit.*, art 5-b.

¹⁸² Règl n°(UE) 2016/679, *op., cit.*, art 5-d.

De plus, seules doivent être traitées « les informations adéquates, pertinentes et nécessaires au regard des objectifs poursuivis »¹⁸³. Une obligation de minimisation s'impose donc. Par exemple, si le NIR s'avère nécessaire pour la gestion de l'activité salariale, il ne pourra être demandé à un candidat à un emploi. Il ne sera demandé au moment d'une embauche ferme. L'employeur doit donc faire preuve de modération dans la nature et le nombre de données personnelles qu'il souhaite collecter. En effet, il faut que la nature des informations collectées soit bien proportionnée à la finalité poursuivie par l'employeur. Ainsi la CNIL a pu considérer que la collecte d'informations relatives à la nationalité d'un candidat à un emploi n'est pas proportionnée pour les opérations de recrutement¹⁸⁴.

Ainsi, une donnée ne doit pas être conservée pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elle est traitée¹⁸⁵. Une durée de conservation précise doit donc être déterminée « non pas en fonction de la finalité générale du traitement mais de chacune des catégories de données collectées »¹⁸⁶. Aucune durée de conservation n'est affectée précisément à chaque dispositif de traitement. Une marge de manœuvre est donc laissée aux employeurs étant entendu que la CNIL est fondée à exercer un contrôle de proportionnalité sur la durée définie et qu'elle préconise dans ses recommandations des durées de conservations maximales¹⁸⁷. L'employeur doit donc être apte à gérer des durées de conservation distinctes et en mesure d'effectuer toute purge ou destruction sélective des données. La programmation d'un algorithme s'avérera alors presque indispensable.

Enfin, une donnée de qualité est une donnée sécurisée. Ainsi, une obligation de sécurité et de confidentialité des données s'impose à l'employeur¹⁸⁸. L'objectif est d'éviter la transmission de données collectées à des tiers non autorisés. Des mesures de sécurité devront être prises. Ces dernières pourront être physiques, c'est-à-dire prévoir un « mécanisme de verrouillage systématique des postes informatiques, des verrous aux portes », ou logistiques en prévoyant « des dispositifs de gestion des habilitations et de contrôle d'accès, de cryptage des

¹⁸³ Règl n°(UE° 2016/679, *op., cit.*, art 5-c.

¹⁸⁴ CNIL, délib.n°2010-112, 22 avr.2010.

¹⁸⁵ Règl n°(UE° 2016/679, *op., cit.*, art 5-e.

¹⁸⁶ G.DESGENS-PASANAU, *op.,cit.*, p.59.

¹⁸⁷ Par exemple, pour les dispositifs de gestion de carrière, le temps de conservation est le temps de présence dans l'entreprise. Elle préconise une durée de deux mois pour les dispositifs de géolocalisation, six mois pour les dispositifs de contrôle des connexions Internet par les salariés, cinq ans pour les données biométriques à compter du départ du salarié de l'entreprise. Pour les dispositifs de vidéosurveillance, la CNIL exige que les images soient supprimées à l'issu d'un délai d'un mois, et de deux ans pour les données collectées lors d'opérations de recrutement après le dernier contact avec la personne concernée.

¹⁸⁸ Règl n°(UE° 2016/679, *op.,cit.*,art 32.

données, ou encore la mise en place de mots de passe complexes et individuels régulièrement changés »¹⁸⁹. Ainsi seules les personnes habilitées en raison de leur fonction peuvent consulter les données personnelles des salariés. L'exemple le plus marquant est la rigueur qu'impose la mise en place du vote électronique dans les entreprises. La sécurité doit la pierre angulaire du dispositif tant en ce qui concerne la régularité du vote que la confidentialité des électeurs¹⁹⁰.

En définitive, afin de protéger les données personnelles des salariés toute collecte de données n'est pas autorisée. Seules certaines catégories de données et certaines collectes sont possibles, sous certaines conditions.

Une fois collectée, tout traitement des données n'est pas non plus permis. C'est également à travers le respect de principes liés au traitement des données que l'exigence cardinale de protection des données est garantie.

§2. La licéité par l'existence de principes liés au traitement des données

Le RGPD, à l'instar de la loi dite « Informatique et libertés » prévoit une liste limitative de conditions sous réserve desquelles un traitement de données personnelles est licite. Si le consentement au traitement était perçu comme le « cœur névralgique » du RGPD¹⁹¹, il s'avère que dans le cadre des relations de travail, ce dernier s'efface (A). Ce retrait du consentement n'a toutefois pas eu pour conséquence de réduire l'intelligibilité du traitement, qui a d'ailleurs été renforcée (B).

A. L'anéantissement du traitement avec consentement

Contrairement aux idées reçues, le RGPD ne modifie pas fondamentalement les différentes conditions de licéité du traitement définies par les réglementations originelles. Ainsi, si pour être licite, le traitement doit avoir reçu le consentement de la personne

¹⁸⁹ F.BARBIER-CHASSAING, « Garantir la sécurité des données et mieux prendre en compte la cybercriminalité dans une logique de responsabilisation pour les entreprises », *Dalloz IP/IT 2019*, p.217.

¹⁹⁰ V. Décret n°2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise ; C.trav., R. 2324-6 à R.2324-15. Un cahier des charges doit être scrupuleusement respecté par l'employeur à savoir : la mise en place d'un « fichier des électeurs » permettant l'authentification des électeurs et un fichier « contenu de l'urne électronique » développant les clés de chiffrement et de déchiffrement; l'exclusivité de l'accès aux données électroniques aux personnes en charge de la gestion et de la maintenance du système de vote; le caractère hermétique et scellé du matériel pendant toute la durée du scrutin et la mise en place d'une assistance technique pour veiller au bon fonctionnement du système. Des tests doivent être réalisés avant le déroulement du vote. Enfin, une expertise préalable par un expert indépendant doit être réalisée avant le scrutin.

¹⁹¹ S.PELLET, « RGPD : l'effacement du consentement », *Revue générale du droit des assurances* - n°01, p.6.

concernée¹⁹², les exceptions prévues à l'article 6-b et 6-f du RGPD permettent de faire échec à cette obligation.

Ces deux exceptions visent le cas du traitement qui est « nécessaire à l'exécution d'un contrat » ou qui est « nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement sous réserve de ne pas méconnaître les intérêts ou les libertés et droits fondamentaux de la personne concernée ». Outre les dispositifs de traitement nécessaire à la réalisation du contrat de travail comme les données RH, l'intérêt légitime poursuivi par l'employeur constitue une base juridique au traitement.

En précisant que cet intérêt légitime ne doit pas méconnaître les intérêts ou les libertés et droits fondamentaux des salariés, le RGPD impose un contrôle de proportionnalité et d'opportunité sur la mise en place desdits dispositifs. Le traitement doit donc être strictement nécessaire à l'intérêt légitime de l'entreprise¹⁹³ et dès lors qu'une autre technique moins attentatoire aux droits et libertés des salariés peut être mise en place, le traitement est alors interdit.

Par exemple, en ce qui concerne les dispositifs de pointeuses biométriques reposant sur une carte à puce individuelle, la jurisprudence a déjà pu considérer que, si sa mise en œuvre permettait de contrôler efficacement les horaires des salariés, d'autres alternatives à la biométrie existaient, de sorte qu'elles devaient être privilégiées¹⁹⁴. Les dispositifs de géolocalisation destinés à contrôler la durée du travail ne sont également licites que si ce contrôle ne peut être opéré par un autre moyen, fût-il moins efficace¹⁹⁵, et lorsque le salarié ne dispose pas d'une liberté dans l'organisation du travail¹⁹⁶. Concernant les dispositifs de vidéosurveillance, si ces derniers répondent à des objectifs sécuritaires comme le contrôle de l'accès aux locaux ou de protection des personnes ou des biens, ils ne peuvent en revanche

¹⁹² Règl n°(UE° 2016/679, *op.,cit.,art 6*.

¹⁹³ C.trav., L.1121-1 : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

¹⁹⁴ TGI Paris, 19 avril 2015 : En l'espèce, il était reproché à la société Effia Services, filiale de la SNCF, d'avoir mis en œuvre un dispositif biométrique de pointage et de contrôle des horaires des salariés. Le tribunal fait une application stricte du principe de proportionnalité en considérant que la mise en place d'un système de badge classique était de « nature à permettre de contrôler efficacement les horaires des salariés sans avoir recours à un procédé d'identification comportant des dangers d'atteinte aux libertés individuelles dont la nécessité n'est pas démontrée ». En analysant d'une part, les avantages attendus pour l'employeur (le contrôle des horaires des salariés) et les risques induits en termes d'atteintes aux libertés pour les personnes concernées, le tribunal a considéré que des technologies alternatives à la biométrie existaient et qu'elles devaient être privilégiées (par exemple, badgeuse classique associé à la frappe d'un code secret). Dans sa décision, le tribunal a par conséquent ordonné purement et simplement l'interdiction d'utiliser le dispositif biométrique en cause.

¹⁹⁵ Cass.soc 18 janvier 2018 n°16-20.618 ; Cass.soc 3 novembre 2011 n°10-18.036 ; CE. 15 décembre 2017, n°403776.

¹⁹⁶ Cass.soc 17 décembre 2014, n°13-23645.

avoir pour seul objectif la mise sous surveillance spécifique d'un employé ou d'un groupé d'employés¹⁹⁷. La prudence de l'employeur dans la justification de la finalité est de mise puisque si l'objectif est d'assurer la sécurité des personnes ou des biens, alors ce système ne pourra servir de preuve pour attester une faute d'un salarié, sauf si la faute se rattache à la vie de l'entreprise¹⁹⁸. De même, une mise sous surveillance constante et permanente dans l'objectif de contrôler l'activité des salariés est interdite et ce, quel que soit le dispositif utilisé¹⁹⁹.

Comme le consentement correspond à « toute manifestation de volonté, libre, spécifique, éclairée et univoque »²⁰⁰, le consentement d'un salarié ne s'inscrit certainement pas dans cette démarche. En effet, le recueil du consentement des salariés est perçu comme une fiction étant donné que le salarié, placé sous la subordination de son employeur, n'exerce pas de réelle liberté de choix. L'exigence du consentement ressemblerait ainsi à un vœu pieux²⁰¹ tant il est inimaginable de penser que les salariés refuseraient de donner leur consentement sous peine de subir un préjudice tel que le fait de se voir refuser un emploi. La CNIL, puis le G29 considèrent en effet qu'il existe un « déséquilibre significatif »²⁰² entre l'employeur et le salarié. Le consentement du salarié ne peut pas alors constituer un fondement juridique valable pour le traitement des données personnelles. Autrement dit, « le lien de subordination intrinsèque à la relation entre un employeur et son salarié risquerait d'invalider le consentement du salarié au traitement de ses données personnelles »²⁰³. L'employeur aura donc tout intérêt à utiliser l'intérêt légitime de son entreprise, plutôt que de faire reposer la licéité de son traitement sur un consentement dont la validité juridique sera certainement retoquée devant l'autorité judiciaire ou la CNIL. Le consentement du salarié sera alors requis que s'il n'est pas

¹⁹⁷ CE, 18 novembre 2015, n°371196 ; CNIL délib n°2014-307, 17 juillet 2014.

¹⁹⁸ Cass.soc; 26 juin 2013, n°12-16.564.

¹⁹⁹ La CNIL a eu l'occasion, à de nombreuses reprises, de considérer que la mise en œuvre d'un dispositif général de contrôle de l'activité des salariés par vidéo-surveillance continue plaçant le personnel sous surveillance constante et permanente (sur toute la durée du travail), était manifestement disproportionnée au regard de la finalité poursuivie par le responsable de traitement. Les dispositifs de géolocalisation des salariés suivent le même régime lorsque la tâche à accomplir par ce salarié réside dans la réalisation d'une prestation pouvant faire elle-même l'objet d'une vérification ou d'une évaluation distincte comme, par exemple, le nombre de ventes réalisées par un représentant de commerce. La CNIL préconise également qu'un dispositif de désactivation du système de géolocalisation puisse être utilisé par le salarié lorsque celui-ci est autorisé à utiliser son véhicule professionnel en dehors de ses heures de travail.

²⁰⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 4.

²⁰¹ Avis du G29, 15/2011 du 13 juill.2011 sur la définition du consentement, WP 187, p.15 ; v. égal. L'avis du G29, WP 48 sur le traitement des données à caractère personnel dans le contexte professionnel.

²⁰² *Ibid.*

²⁰³ J.SCHWARTZ, « Le point sur le RGPD : nouvelles obligations, nouveaux enjeux », *Les Cahiers Sociaux* – n°306, p.228.

nécessaire à l'intérêt légitime de l'entreprise²⁰⁴ comme par exemple, l'utilisation de la photographie d'un salarié à des fins publicitaires.

En somme, si le consentement est apparu comme « l'épicentre » des garanties assurant la protection des données personnelles, il s'avère que les exceptions précitées anéantissent et vident le consentement de sa substance. Considéré comme l'élément clef de la protection des données personnelles, sa place a été surestimée. En effet dans les relations de travail, le consentement n'est une condition ni systématique, ni suffisante de la licéité d'un traitement des données. Cependant, le législateur a particulièrement veillé au grain en assujettissant pareille licéité à des obligations rigoureuses, ersatz du consentement.

B. Le renforcement des règles d'intelligibilité du traitement

Si les nouvelles technologies offrent à l'employeur de nombreux dispositifs de traitement des données personnelles, quels que soient les dispositifs mis en place dans l'entreprise, l'employeur doit au préalable informer les salariés²⁰⁵. A défaut d'information, le traitement de données issu de ces dispositifs sera illicite et ne pourra pas constituer un moyen de preuve licite²⁰⁶. La récusation des moyens de preuve est possible, ce qui pourrait devenir primordial pour la suite (et le bien-fondé) de la procédure disciplinaire.

Cette information, effectuée par le biais d'une notice d'information, doit comporter plusieurs informations, selon que les données sont collectées directement²⁰⁷ ou indirectement auprès du salarié²⁰⁸.

Par exemple, en ce qui concerne les enregistrements ou écoutes téléphoniques, la CNIL exige que les salariés dont les conversations sont susceptibles d'être enregistrées soient précisément informés des conditions d'enregistrement (y compris les interlocuteurs au moyen d'un message vocal). En ce qui concerne les dispositifs de géolocalisation, puisque le consentement du salarié n'est pas envisageable, la CNIL se limite à exiger que le salarié soit informé des modalités exactes du fonctionnement du dispositif de géolocalisation. Pour les

²⁰⁴ C.SCHULTIS, « Le traitement de données dans le cadre des relations de travail dans le règlement sur la protection des données personnelles », *Dalloz IP/IT*, 2017, p. 265.

²⁰⁵ C.trav., L.1121-1 ; L.1222-4.

²⁰⁶ Cass.soc; 22 mai 1995, n°93-44.078 ; Cass.soc.; 20 novembre 1991, n°88-43.120.

²⁰⁷ Règl.n°(UE) 2016/679, *op.,cit.*, art 13. A ce titre, l'information doit comprendre l'identité et les coordonnées de l'employeur (représentant ou DPD), les finalités du traitement, l'existence ou pas d'une prise de décision automatisée, l'accès à leurs droits, et le caractère réglementaire ou contractuel des informations exigées.

²⁰⁸ Règl.n°(UE) 2016/679, *op.,cit.*, art 14. A ce titre, si les données sont collectées indirectement auprès d'organismes tiers (comme les données collectées via l'URSSAF ou le Trésor public), la notice doit indiquer, outre les données précitées, les catégories de données collectées indirectement et la source de leur provenance.

dispositifs de cybersurveillance des salariés, la CNIL recommande de porter à la connaissance des salariés le principe retenu pour différencier les e-mails professionnels des e-mails personnels (qualification de l'objet, création d'un répertoire spécifique dédié au contenu privée).

Si les règles d'intelligibilité du traitement des données personnelles des salariés sont clairement définies, il en est autrement pour les candidats à un emploi où l'obligation d'information relève souvent de l'utopie. Concernant les opérations de recrutement, l'article L.1221-8 du Code du travail prévoit que « le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard ». L'employeur doit également informer le candidat, non seulement de l'issue donnée à sa candidature, mais également de la durée de conservation des informations le concernant, ainsi que la possibilité de demander la restitution ou la destruction desdites informations. La CNIL recommande d'ailleurs que l'information concernant les données de recrutement soit dispensée préalablement par écrit.

Ainsi, si l'employeur n'a pas besoin de recueillir le consentement du salarié sur le traitement de ses données, il doit en revanche se contraindre à lui fournir une information claire et précise.

Afin de rendre davantage intelligible le traitement des données, l'employeur devra également informer et consulter la collectivité de travail à travers leurs représentants.

Le Conseil social et économique devra donc être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens et techniques permettant un contrôle de l'activité des salariés²⁰⁹. L'absence de consultation obligatoire par l'employeur rend, d'une part les modes de preuves illicites²¹⁰, et d'autre part expose l'employeur à des sanctions pénales pour délit d'entrave²¹¹.

Si l'avis du CSE n'est que consultatif et ne lie pas l'employeur, ces obligations montrent que le législateur a souhaité rendre totalement transparent les dispositifs de traitements des données personnelles telles que l'exigent les dispositions de l'article 5-a du RGPD. Malgré l'absence du consentement, cette transparence permet aux salariés de maîtriser, dans une certaine mesure, leurs données.

²⁰⁹ C.art., L.2312-38.

²¹⁰ Cass.soc 7 juin 2006, n°04-43.866.

²¹¹ C.art., L.2317-1.

En définitive, l'obligation d'information et de consultation permet de rendre intelligible, à condition qu'elle soit claire et précise, et la consultation utile, l'intégralité du cycle de vie des dispositifs de traitements de données personnelles. Si cette obligation peut paraître opportune, elle peut aussi devenir source de complexité inutile pour les entreprises. En effet ces obligations peuvent relever du casse-tête tant les données collectées sont nombreuses, de natures diverses et soumises à des règles de finalité et de conservation différentes. Ce faisant, il y a fort à parier que le résultat sera probablement strictement inverse à l'effet recherché.

Ainsi, comme cela a été expliqué, si des principes relatifs tant à la collecte qu'au traitement des données personnelles irriguent la licéité du dispositif mis en place par l'employeur, il en ressort que le RGPD n'a introduit que quelques nouveaux concepts. Dans un contexte de concurrence exacerbée, il reste à voir comment la nouvelle réglementation RGPD assure l'effectivité de la protection des données personnelles des salariés à l'égard des traitements opérés par les entreprises.

Section 2 – L'examen de l'effectivité

Le RGPD provoque une rupture profonde dans la logique qui régnait dans la réglementation « Informatique et libertés ». Le mécanisme des formalités préalables se voit remplacé par un système d'auto-contrôle des entreprises. Malgré ce changement de cap, l'objectif est de maintenir un niveau élevé de protection des données personnelles. Ainsi, pour assurer l'effectivité du nouveau mécanisme de protection, il est apparu nécessaire de moderniser la maîtrise des salariés sur leurs données personnelles (§1) tout en adaptant les garants de la protection (§2).

§1. La modernisation de la maîtrise des données transmises

En considérant que les personnes concernées par les dispositifs de traitement sont les plus à même d'assurer la protection de leurs données personnelles, le RGPD opère une révolution culturelle en rendant les salariés véritablement acteur. A ce titre, le RGPD confirme les droits d'intervention du salarié sur ses données (A) et se veut novateur en consacrant de nouveaux droits (B).

A. La confirmation des droits existants

Le RGPD vient confirmer toute une série de droits dont disposait le salarié sur ses données personnelles. Les salariés conservent donc leurs droits d'accès²¹², de rectification²¹³ et d'opposition²¹⁴. Etant des « droits strictement personnels »²¹⁵, c'est au salarié de demander à l'employeur d'exercer ces droits. Le mandat n'est donc pas admis, sauf pour les mineurs ou les incapables majeurs conformément au droit commun.

Tout salarié ou ancien salarié peut donc demander à son employeur (ou ancien) d'accéder aux données personnelles le concernant qui ont été collectées, les finalités du traitement, les destinataires de ces données, leur durée de conservation etc. En pratique, il demandera au Directeur des ressources humaines d'accéder aux données relatives à son recrutement, son historique de carrière, sa rémunération, l'évaluation de ses compétences professionnelles comme les entretiens annuels d'évaluations, ses notations ou encore son dossier disciplinaire. Le salarié a donc accès à l'intégralité des données personnelles le concernant qu'il s'agisse de « données « brutes » comme le nom, l'adresse, les avertissements, mais également à toutes les informations qui lui sont indirectement reliées comme les codifications, les segmentations ou les zones blocs-notes »²¹⁶.

L'employeur doit faire droit à sa demande. Le salarié n'a pas à justifier d'une quelconque raison. Il n'a donc pas besoin de motiver sa demande. Afin de rendre effectif ce droit, le RGPD a raccourci le délai de réponse de l'employeur à un mois²¹⁷ (lequel était auparavant de deux mois). En cas de refus d'accéder à la demande du salarié, l'employeur devra motiver sa réponse tout en précisant les voies et les délais de recours ouverts. En cas de réponse positive, le salarié obtiendra une copie de ses données sous format papier, et fait nouveau, la copie pourra être fournie sous une forme électronique facile d'accès (clé USB, courrier électronique) si le salarié en fait la demande par voie électronique.

Le droit d'accès aux données personnelles n'a pour ambition que de permettre au salarié dont les données sont traitées, de pouvoir les rectifier. Ce droit de rectification apparaît alors

²¹² Règl.n°(UE) 2016/679, *op., cit.*, art 15 ; Loi n°78-17, 6 janv.1978, art 39 mod.par L.2018-493,20 juin 2018, *op.,cit.*

²¹³ Règl.n°(UE) 2016/679, *op.,cit.*, art 16 ; Loi n°78-17,6 janv.1978, art 40 mod. par L.2018-493,20 juin 2018, *op.,cit.*

²¹⁴ Règl.n°(UE) 2016/679, *op., cit.*,art 21 ; Loi n°78-17,6 janv.1978, art 38 mod. par L.2018-493,20 juin 2018,*op.,cit.*

²¹⁵ G.DESGENS-PASANAU, *op.,cit.*, p.101.

²¹⁶ *Ibid.*

²¹⁷ Règl.n°(UE) 2016/679, *op.,cit.*, art 12.3.

comme le prolongement nécessaire du droit d'accès aux données²¹⁸. En ce sens, les salariés ont le droit d'obtenir de l'entreprise, dans les meilleurs délais, la rectification des données personnelles inexactes les concernant. Le salarié pourra donc demander que les données inexactes soient corrigées ou complétées, et à ce que les traitements des données concernées soient verrouillés jusqu'à régularisation. En ne précisant pas de délai, le législateur a souhaité laisser une certaine souplesse aux entreprises pour décider de l'opportunité (mais surtout de la faisabilité) du délai de rectification, sous couvert de respecter le traditionnel délai raisonnable.

Ainsi, le RGPD confirme la collaboration qui doit s'opérer entre l'employeur et le salarié sur l'exactitude des données personnelles de ce dernier. Conscient que les entreprises, notamment les TPE-PME, puissent éprouver des difficultés à assurer l'exactitude des données qui évoluent constamment, le RGPD continue de faire contribuer le salarié, considéré comme le mieux placé pour s'en assurer.

Même si l'employeur n'a pas besoin de recueillir le consentement du salarié, ce dernier dispose d'un droit d'opposition sur le traitement de ses données personnelles, notamment s'il conteste la légitimité des motifs poursuivis par l'employeur. Ce droit d'opposition peut se rapprocher de la notion de consentement au traitement²¹⁹ étant donné que si l'employeur démontre qu'il existe des « motifs légitimes et impérieux pour le traitement », prévalant sur les intérêts et droits et libertés des salariés, ou pour la « constatation, l'exercice ou la défense de droits en justice », l'employeur pourra alors poursuivre le traitement. Si ce droit d'opposition pourrait théoriquement constituer un rempart face au traitement de données personnelles non désirées, il y a fort à parier que l'opposition des salariés cède fréquemment face aux obligations légales de l'employeur et face à l'intérêt légitime de l'entreprise.

En définitive, le RGPD vient confirmer les droits traditionnels existants dans la réglementation « Informatique et libertés » originelle. Cependant, afin d'adapter le cadre juridique au progrès numérique et technologique, le RGPD est venu consacrer deux nouveaux droits, à savoir le droit à l'oubli et à la portabilité des données personnelles.

²¹⁸ F. EL ATMANI, « La protection des données personnelles dans l'Union européenne », Thèse de droit privé soutenue à la faculté de Montpellier, 1996, p.121.

²¹⁹ C.CASTETS-RENARD, « La protection des données personnelles dans les relations internes à l'Union européenne – La protection des données personnelles en matière civile et commerciale », 2018 (actualisation : Mai 2019), p.126.

B. La consécration de nouveaux droits

Le droit à la portabilité des données, bien que redouté par les entreprises, est un des éléments essentiels du nouveau dispositif. Le salarié a le droit de récupérer les données collectées dans un format facilement réutilisable et lisible, et de les réutiliser à des fins personnelles²²⁰. Cependant ce droit est assorti de deux conditions.

La première concerne le champ d'application puisque le texte prévoit que ne pourront faire l'objet d'un droit à la portabilité « que les données des personnes concernées qui ont été fournies au responsable de traitement ». Concernant ce critère, certains ont pu considérer qu'il s'agissait uniquement des données délibérément fournies par le citoyen-salarié. Or, pour le G29²²¹, si ces données concernent effectivement celles « fournies activement et délibérément »²²² par les salariés, elles englobent également les « données générées et collectées à partir de leurs activités par l'utilisation d'un dispositif de traitement des données utilisé »²²³ par l'employeur. Si de prime abord cette condition paraissait restrictive, il s'avère qu'elle permet de prendre en compte presque l'intégralité des données traitées dans le cadre de la relation de travail.

La deuxième condition est quant à elle restrictive. Elle tient au fondement de licéité du traitement puisqu'il ne pourra s'agir que de traitements réalisés sur la base du consentement ou sur l'exécution du contrat. Pour les salariés, le consentement étant exclu, seuls les traitements fondés sur l'exécution du contrat de travail permettront l'exercice du droit à la portabilité.

Ainsi avec ce nouveau droit, le salarié obtiendra une copie de ces données « dans un format structuré, couramment utilisé et lisible par machine » et pourra les faire transférer, « si cela est possible techniquement, » directement chez un autre employeur. A ce titre, le RGPD favorise les transferts des dossiers des salariés dans un contexte où les restructurations des entreprises sont monnaies courantes. Le refus de l'octroi de ce droit sur une autre base légale que celle de l'exécution du contrat ou du consentement en est une caractéristique. Or comme il a été précédemment démontré, l'anéantissement du consentement limite la portée de ce droit²²⁴. De même, à court terme, sa mise en œuvre apparaît difficile pour les TPE-PME puisque

²²⁰ Règl.n°(UE) 2016/679, *op.,cit.*, art 20.

²²¹ [Communiqué G29] Séance plénière du G29 des 12 et 13 décembre 2016.

²²² *Ibid.*

²²³ *Ibid.*

²²⁴ Sauf à imaginer que le consentement retrouve un second souffle en cas de départ volontaire du salarié de l'entreprise.

« les entreprises devront définir des standards juridiques et techniques permettant un minimum d'interopérabilité entre les différents systèmes informatiques des entreprises »²²⁵.

Concernant le droit à l'effacement ou le droit à l'oubli (« *right to be forgotten* »), le RGPD²²⁶ vient renforcer l'utilisation de ce droit, fort médiatisé depuis l'arrêt Google Spain²²⁷. Le salarié a le droit de demander à l'entreprise d'effacer, dans les meilleurs délais, l'ensemble des données collectées, dans la limite des obligations légales, du caractère d'intérêt général du traitement des données, sauf si le traitement est nécessaire dans le cadre d'un procès. Ce droit n'est pas inconditionnel puisqu'il est assorti de plusieurs conditions devant être au préalable remplies. Ainsi, l'employeur devra faire droit à la demande du salarié si les données personnelles le concernant ont fait l'objet d'un traitement illicite, s'il n'existe pas de motifs légitimes et impérieux et si les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Autrement dit, par principe la demande d'effacement est valable, à moins que le responsable de traitement ne trouve une raison valable pour s'y opposer. A titre d'illustration, une entreprise utilisant un « intranet de recrutement peut être amenée à répondre à une demande d'une personne souhaitant faire disparaître l'accès à son profil parce qu'il dispose d'un classement peu avantageux. Or l'intérêt de l'employeur est de pouvoir disposer d'une visibilité de l'ensemble de ses salariés pour assurer au mieux sa gestion et son efficacité »²²⁸.

De lege data, ce droit à l'oubli n'est pas véritablement nouveau et les critiques surgissent déjà qualifiant son apparition de « phénomène cosmétique et regrettant l'occasion manquée d'aller plus loin »²²⁹. En effet, s'il est possible au salarié de demander l'effacement de ses données personnelles, en revanche ce droit à l'oubli n'est pas synonyme de droit au déréférencement. Les données seront effacées des bases de données de l'employeur mais les liens des moteurs de recherche ne seront pas effacés, permettant alors la réidentification du salarié.

²²⁵ G.DESGENS-PASANAU, *art., préc.* p.97.

²²⁶ Règl.n°(UE) 2016/679, *op., cit.*, art 17 ; Loi n°78-17,6 janv.1978, art 40 II mod. par Loi.n°2018-493,*op., cit.*

²²⁷ CJUE, 13 mai 2014, Google Spain, aff. C-131/12.

²²⁸ « Le traitement des données à caractère personnel », Dictionnaire Permanent Social, Editions législatives.

²²⁹ G.DESGENS-PASANAU, « RGPD : entre incertitudes et occasions manquées », *Dalloz IP/IT*, 2016, p. 335.

S'y ajoute un nouveau droit à la limitation du traitement²³⁰. Perçu comme une sorte de « droit allégé »²³¹ à celui de l'effacement des données, il permet au salarié d'obtenir la suspension de l'utilisation des données par l'employeur notamment lorsque les données sont inexactes et/ou le traitement illicite. Ce droit offre ainsi la possibilité pour le salarié d'obtenir la suspension temporaire de l'accès à ses données, dès qu'il a formulé une demande d'effacement, pendant la durée du processus de traitement de la demande, et même si celle-ci sera finalement refusée. Ce droit est redoutablement efficace pour le salarié qui utilise ce droit d'effacement sans avoir à supporter de délai d'attente qui peut être très long, même si le RGPD le limite théoriquement à un mois.

En somme, la confirmation et la consécration de ces droits visent à assurer le renforcement du « contrôle que les personnes concernées exercent sur leurs propres données »²³². Si la volonté de remettre le citoyen-salarié au centre du RGPD est bel et bien présente, il reste à voir si ces derniers seront des acteurs de premier plan ou alors de simples spectateurs dans la protection de leurs données personnelles.

Cette nouvelle logique de responsabilisation a eu aussi pour conséquence de renforcer et d'adapter le rôle des garants de la protection des données personnelles.

§2. L'adaptation des garants de la protection des données

Pour pallier la suppression du mécanisme de contrôle a priori, le RGPD met les responsables de traitement à contribution en les faisant devenir les gardiens du nouveau régime de protection (A). Toutefois, le garant d'une régulation respectueuse des droits et libertés fondamentaux des salariés demeurant la CNIL, il est nécessaire qu'elle puisse disposer de moyens nécessaires lui permettant de jouer le rôle de clef de voûte de ce nouveau régime (B).

A. Le responsable de traitement comme gardien du régime de protection

Le responsable de traitement est placé en première ligne. Comme ce dernier n'a plus de formalités préalables à accomplir auprès de la CNIL, les employeurs se voient contraints de respecter toute une série d'obligations visant à assurer la conformité du traitement au

²³⁰ Règl.n°(UE) 2016/679, *op.,cit.*,art 18.

²³¹ G.DESGENS-PASANAU, « La protection des données personnelles, le RGPD et la loi française du 20 juin 2019 », LexisNexis, 2019, p.99.

²³² Règl.n°(UE) 2016/679, *op.,cit.*,considérant 68.

règlement. Cette « check list » d'outils de conformité se traduit par des actions de nature à la fois juridique, technique et organisationnelle²³³.

L'anticipation étant le mot d'ordre, c'est en amont du traitement que la majorité des actions de conformité se réaliseront. Cette logique de conformité (ou « compliance ») impose que la protection des données personnelles ait lieu dès la conception (« privacy by design ») et par défaut (« privacy by default »), mais également de manière continue. Les employeurs devront être en mesure de démontrer cette mise en conformité à tout moment (« accountability »)²³⁴.

L'employeur devient donc « acteur et responsable de sa mise en conformité et en supporte la charge de la preuve »²³⁵. Concrètement, il est attendu de l'employeur qu'il tienne une documentation (tenue d'un registre), qu'il mette en œuvre des obligations de sécurité, qu'il réalise une analyse d'impact relative à la protection des données et qu'il prenne en compte les risques particuliers (gestion des risques).

La tenue d'un registre par le responsable de traitement succède donc aux « fichiers des fichiers » tenus par les autorités de contrôle²³⁶. Obligatoire pour les entreprises de plus de 250 salariés, ou celles ayant des activités susceptibles de présenter des dangers²³⁷, ce nouveau registre perd son caractère public puisqu'il est seulement mis à la disposition des autorités de contrôle, et n'est donc pas accessible à tous, contrairement « aux fichiers des fichiers »²³⁸.

En application du principe de « privacy by design », c'est notamment au travers de la réalisation d'une étude d'impact que l'employeur démontrera que la protection des données personnelles a été anticipée dès la conception du dispositif. En cas de risque élevé, il devra toutefois consulter la CNIL. Obligatoire que lorsque le traitement répond à au moins deux conditions fixées par le RGPD²³⁹, il est regrettable que les entreprises sur lesquelles

²³³ A.DEBET, « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p.592.

²³⁴ Règl.n°(UE) 2016/679, *op.,cit.*, art 25.

²³⁵ C.CASTETS-RENARD, « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p. 331.

²³⁶ Directive 95/46/CE, *op., cit.*, art 21.

²³⁷ Règl.n°(UE) 2016/679, *op.,cit.*, art 30.5.

²³⁸ Règl.n°(UE) 2016/679, *op., cit.* art 30.4.

²³⁹ Les conditions à respecter sont les suivantes : « évaluation/scoring (y compris le profilage), décision automatique avec effet légal ou similaire, surveillance systématique, collecte de données sensibles ou données à caractère hautement personnel, collecte de données personnelles à large échelle, croisement de données, personnes vulnérables (patients, personnes âgées, enfants, etc.), usage innovant (utilisation d'une nouvelle technologie), exclusion du bénéfice d'un droit/contrat ».

l'obligation de mener une étude d'impact ne soient pas clairement identifiée²⁴⁰. Or, cette approche fondée sur le risque peut être à déplorer²⁴¹ car l'employeur n'est surement pas le mieux placé pour décider de l'opportunité de la réalisation d'une étude d'impact.

Puisque l'employeur ne dispose pas toujours des compétences adéquates en matière de données personnelles, le RGPD prévoit l'obligation pour certains de désigner un délégué à la protection des données, feu le correspondant informatique et libertés (CIL). Garant du respect de la réglementation, il sera « vecteur de sécurité juridique »²⁴² puisqu'il sera le référent d'une part, en matière d'identification et de coordination des actions à mener, et d'autre part, sur toutes les questions des salariés et employeurs relatives aux données personnelles. Sa désignation n'est pas obligatoire en fonction de la taille de l'entreprise mais des données traitées²⁴³ par elle. Auparavant la désignation du CIL était facultative, ce qui montre le souci d'assurer la protection des données personnelles en fonction des situations données. Il y a donc une « individualisation dans sa désignation »²⁴⁴. Indépendant²⁴⁵, l'employeur ne doit pas lui donner des instructions ni le sanctionner pour l'exercice de ses missions²⁴⁶. Toutefois, le RGPD est silencieux sur les garanties statutaires dont bénéficierait le DPD propres à assurer son indépendance. Il serait opportun de lui faire bénéficier d'un statut et d'une protection similaire à ceux des salariés protégés²⁴⁷. Aussi, il est loisible de penser que le rapport de force ne leur est pas favorable. De même, si l'avancée est notable, elle est selon certains insignifiante²⁴⁸ puisque, s'il est désigné sur la base de ses qualités professionnelles, notamment ses connaissances spécialisées, aucune formation obligatoire n'est prévue. Compte tenu de la complexité de la matière, il aurait été souhaitable qu'il bénéficie d'un minimum d'heures de formation.

²⁴⁰ C.FERAL-SCHUHL, « Des obligations des responsables de traitement renforcées », *Cyberdroit*, 2018-2019.

²⁴¹ Règl.n°(UE) 2016/679, *op.,cit.* art 35.1

²⁴² G.DESGENS-PASANAU, *art., préc.*, p.139

²⁴³ Règl.n°(UE) 2016/679, *op.,cit.*, 37.1. Pour les entreprises, la désignation est obligatoire lorsque « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées (ici, il s'agit des dispositifs de surveillance comme la géolocalisation, vidéosurveillance) ; ou lorsque les activités consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 (ici, il s'agit notamment des traitements de données sensibles) ».

²⁴⁴ C.CASTETS-RENARD, « Les enjeux et l'actualité de la protection des données personnelles en Europe », Larcier, « Quelle protection des données personnelles en Europe ? », 2015, p.37.

²⁴⁵ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *art., préc.*

²⁴⁶ Règl.n°(UE) 2016/679, *op.,cit.*, art. 38, al. 3.

²⁴⁷ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *op.,cit.*

²⁴⁸ C.CASTETS-RENARD, *art.,préc.*, p.38.

En se détachant des mesures systématiques, ces outils de conformité sont pertinents puisqu'ils vont permettre une gestion plus précise et individualisée des traitements des données. S'il est certain que les grandes entreprises ne rencontreront pas de difficultés dans la mise en œuvre d'une politique de gestion et de contrôle des risques, il en est autrement pour les TPE-PME, non aguerries à ce type de pratiques.

Aussi, le passage d'un régime de protection fondé à un mécanisme d'autocontrôle et de responsabilisation des employeurs implique nécessairement l'existence d'une autorité de contrôle propre à assurer sa mission de protection des données personnelles. La CNIL apparaît alors comme la pierre angulaire de ce nouveau régime de protection

B. La CNIL comme clef de voûte du régime de protection

Le progrès numérique et technologique a rendu impossible le respect de la législation en un seul contrôle instantané opéré par la CNIL. Le RGPD a donc supprimé le dépôt de formalités préalables en réaction à la nécessité d'assurer une vigilance continue et dynamique. En tant qu'autorité de régulation, les missions et pouvoirs²⁴⁹ de la CNIL ont dû être renforcés afin d'assurer pleinement sa mission de conseil et de contrôle des entreprises.

Tout d'abord, son rôle d'accompagnement a été renforcé. Cette AAI sensibilise le public et l'entreprise, établit et publie des lignes directrices, des recommandations, des référentiels et des clauses contractuelles types, destinées à faciliter la mise en conformité des traitements de données personnelles et à procéder à l'évaluation préalable des risques²⁵⁰. Elle encourage les entreprises à élaborer des codes de conduites ou des chartes destinées à favoriser la conformité des traitements. Elle reçoit les réclamations, pétitions et plaintes des salariés ou des syndicats et présente, chaque année, un rapport au Président de la République et au Parlement. La CNIL conserve donc ses missions d'information et de conseil, la principale nouveauté tient au fait que ses missions ont été élargies puisqu'elles s'étendent désormais aux sous-traitants.

Conseillère des entreprises et des salariés, elle l'est également pour les institutions normatives. Sa fonction de consultation est ainsi renforcée : elle peut dorénavant être consultée sur toute proposition de loi portant sur la protection des données personnelles par les Présidents

²⁴⁹ Le RGPD dénombre 22 missions (art 57) et 28 types de pouvoirs (art 58) tout en précisant que ces dispositions ne sont pas exhaustives puisque les autorités peuvent « s'acquitter de toutes autres missions relative à la protection des données personnelles » et permettant aux Etats membres de prévoir des pouvoirs additionnels pour ces autorités.

²⁵⁰ Loi n°78-17,6 janv.1978, art 11, 1 1° mod par L.2018-493,20 juin 2018 : JO, 21 juin.

ou les commissions compétentes de l'Assemblée nationale ou du Sénat, et par les présidents des groupes parlementaires²⁵¹.

Dans sa mission de contrôle, son pouvoir d'enquête a été amélioré. A ce titre, elle dispose d'un pouvoir de contrôle permettant à ses membres d'accéder, sous certaines conditions²⁵², aux locaux de l'entreprise. Si les responsables des locaux exercent leur droit d'opposition²⁵³, la visite ne peut se dérouler qu'après autorisation du juge des libertés du TGI dans le ressort duquel sont situés les locaux à visiter. Pour que leur contrôle puisse être efficace, les agents peuvent recueillir sur place, sur convocation, ou en ligne, tout renseignement et toute justification jugés utiles et demander communication de tout document nécessaire à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Sur la forme le changement est radical puisque contrairement à l'ancienne législation, le secret professionnel ne pourra plus leur être opposé, sauf bien sûr les informations couvertes par le secret professionnel applicables aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques et par le secret médical²⁵⁴. L'effectivité des contrôles en ligne sont renforcés puisque les agents de la CNIL peuvent utiliser une identité d'emprunt²⁵⁵.

Enfin, son pouvoir de sanction est sensiblement renforcé. Si la CNIL pouvait, outre retirer une certification ou un agrément en cas de violation des règles sur la protection des données²⁵⁶, donner des rappels à l'ordre, avertissements, mises en demeure parfois sous astreintes, injonctions de cessation du traitement automatisé²⁵⁷, son pouvoir de sanction pécuniaire prend un autre tournant.

²⁵¹ Cons.const.,n °2018-765 DC, du 12 juin 2018.

²⁵² Peuvent accéder de 6 heures à 21 heures, à tous les lieux, locaux, enceintes, installations ou établissement servant à la mise en œuvre d'un traitement de données personnelles (à l'exclusion des parties de ceux-ci affectées au domicile privé), sous réserve d'en informer préalablement le procureur de la République territorialement compétent et le responsable des lieux qui peut s'opposer à cette visite. A noter que lorsque l'urgence, la gravité des faits ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en soit informé, sur autorisation préalable du juge des libertés.

²⁵³ Si les responsables des locaux n'ont pas été informés de leur droit de s'opposer à ces visites, l'entreprise est fondée à soutenir que la sanction qui lui a été infligée, en raison du manquement à la loi « informatique et libertés », dès lors qu'elle reposait sur les lieux constatés lors des contrôles effectués, a été prise au terme d'une procédure irrégulière et doit être annulée (v. CE.,6 novembre 2009, n°304300).

²⁵⁴ Art. 44 de la *LIL* modifié par l'art. 5.

²⁵⁵ Décret n°2018-687 du 1^{er} aout 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

²⁵⁶ Art. 45 t 46 de la *LIL*, *op.,cit.*.

²⁵⁷ En cas d'urgence et de menaces pour les libertés, la CNIL pouvait, après une procédure contradictoire, décider de l'interruption de la mise en œuvre du traitement ou le verrouillage de certaines données traitées pour une durée maximale de trois mois, sans pouvoir toutefois procéder à une destruction.

Outre la possibilité de rendre public ses avertissements – considérée comme la sanction la plus dévastatrice pour les entreprises puisqu'elle impacte son image et peut lui causer un préjudice commercial ou financier important²⁵⁸ – en « complément ou à la place de ces mesures correctrices »²⁵⁹, la CNIL peut condamner les entreprises à une amende administrative dont le montant dépend d'un certain nombre de critères : nature de la violation et des données en cause, caractère intentionnel ou non de l'auteur de la violation, avantages financiers tirés de cette violation, niveau de coopération avec les autorités de contrôle.

Or, c'est faisant fi du pouvoir de sanction pécuniaire relativement faible de la CNIL sous l'ancienne législation²⁶⁰, que les législations qui se sont succédées ont renforcé les sanctions pécuniaires au regard des capacités financières des entreprises. Ainsi, si la loi du 7 octobre 2016 pour une République numérique²⁶¹ avait plafonné les sanctions à trois millions d'euros, le RGPD, conscient du caractère dérisoire, va encore plus loin puisque l'amende administrative peut s'élever à 20 millions d'euros ou 4% du chiffre d'affaire mondial total de l'exercice précédant (le montant le plus élevé des deux devant être retenu)²⁶². Pareille aggravation des sanctions permet d'assurer « la crédibilité et l'effectivité de l'encadrement des responsables de traitement, en particulier s'agissant des grosses structures »²⁶³.

Force est de constater que si la CNIL a démultiplié ses contrôles sur place au cours des dernières années²⁶⁴, les statistiques concernant les sanctions pécuniaires restent souvent décevantes même si un progrès est en cours²⁶⁵.

Pour conclure, le passage d'un régime de protection a priori à un régime de protection a posteriori exige que la CNIL dispose de moyens propres à assurer sa mission d'encadrement

²⁵⁸ Lorsque la Société Acadomia a fait l'objet en 2011 d'un avertissement public pour le fichage illicite des intervenants et pour la présence de commentaires excessifs voire injurieux dans leurs fichiers clients, son cours de bourse a perdu près de la moitié de sa valeur. V. G.DESGENS-PASANAU, *op.,cit.*,p.116.

²⁵⁹ Règl.n°(UE) 2016/679, *op.,cit.*, art 83.

²⁶⁰ Délib.CNIL n°2017-009, 15 juin 2017 : la CNIL a condamné une société à une sanction pécuniaire de 1 000 euros pour avoir installé un système de vidéosurveillance à l'insu de ses salariés et sans déclaration préalable, qui permettait de visualiser en temps réel les images et qui n'assurait pas une sécurité suffisante des données personnelles accessibles.

²⁶¹ Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, art.65.

²⁶² Règl.n°(UE) 2016/679, *op., cit.*, art 83.5.

²⁶³ Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *art.,préc.*

²⁶⁴ P.JANUEL, « CNIL et RGPD : retour sur une année de transition », *Dalloz actualité*,19 avril 2019.

²⁶⁵ Aux termes de son dernier rapport d'activité publié en avril 2019, celle-ci a reçu un nombre record de 11 077 plaintes, ce qui représente une hausse de 32% en un an dont 73% sont liées au non-respect de l'exercice d'un droit. En 2018, elle a réalisé 310 contrôles dont 204 sur place, 51 en ligne et 51 sur pièces. Elle a prononcé 49 mises en demeure et a prononcé 11 sanctions pécuniaires (comme en 2006 au moment de la mise en œuvre des pouvoirs de sanctions de la CNIL) contre 3 sanctions en 2015. Si depuis l'entrée en vigueur du RGPD le nombre de plaintes déposées a augmenté, la CNIL n'a pour l'instant prononcé aucune sanction pour non-respect du règlement. La présidente de la CNIL, Madame Marie-Laure Denis, a annoncé vouloir muscler son action répressive en mettant fin à la « période d'observation et de tolérance» laissée aux entreprises.

et de conseil aux employeurs, d'une part, et dispose d'un pouvoir de sanction dissuasif, d'autre part. Si toutes ces dispositions ne sont pas nouvelles, de nouvelles attributions sont créées et le RGPD renforce indubitablement les pouvoirs de la CNIL. La crédibilité et légitimité de la CNIL reposent désormais sur les pouvoirs de sanctions a posteriori, à charge pour elle de s'en emparer, à défaut de quoi le niveau global de protection des données personnelles des salariés pourrait bien diminuer.

CONCLUSION DU CHAPITRE II

L'entrée en vigueur du RGPD n'a donc pas fait d'ombre à la volonté de préserver les salariés de l'implantation croissante des nouvelles technologies dans l'entreprise puisque des conditions précises sont toujours exigées²⁶⁶.

Le RGPD renouvelle les moyens de protection des données personnelles en envisageant leur licéité comme leur effectivité.

La licéité innerve l'intégralité du processus de saisissement des données personnelles par l'employeur, de leur collecte à leur traitement. Au registre de la collecte, la nature et la qualité des données collectées constituent les pivots de la licéité. Au registre du traitement, outre l'exigence d'un intérêt légitime ou d'une obligation légale, la licéité gravite autour des obligations d'information et de consultation, ersatz le consentement des salariés.

L'effectivité de la protection ne repose plus sur le contrôle a priori opéré par la CNIL. La suppression du mécanisme de formalités préalables s'accompagne d'une part, d'un renforcement des droits des salariés sur leurs données, et d'autre part, d'une responsabilisation accrue des entreprises dans les mécanismes de protection.

Au bénéfice procuré par cette coopération renforcée, s'ajoute une profonde évolution du rôle de la CNIL, dont l'effet désormais dissuasif des sanctions prononcées, est à saluer.

²⁶⁶ G.HAAS, « Bilan après neuf mois d'application du RGPD », *Dalloz IP/IT*, 2019, p.357.

CONCLUSION PARTIE I

La démocratisation et la banalisation du numérique et des technologies au sein de l'entreprise a eu pour conséquence d'inonder les diverses possibilités de collectes et de traitements de données personnelles des salariés, le premier phénomène répondant au second. L'accroissement des dispositifs de traitements a donc soulevé la question de sa compatibilité avec le maintien des droits et libertés fondamentaux des salariés.

Dans cette perspective, les conceptions de vie privée et de données personnelles s'épousent partiellement. L'enjeu de la protection ne se limite pas au respect de la vie privée et recouvre tous les droits et libertés fondamentaux des salariés. La protection des données personnelles s'analyse alors comme un bouclier contre les éventuelles atteintes opérées par les entreprises.

Mais à d'autres occasions, l'intérêt de l'entreprise justifie que l'on fasse fi de cette protection et vient ici renforcer et légitimer le pouvoir de l'employeur dans la détermination des outils et méthodes de travail. Ce pouvoir n'est pas absolu. Il est apparu nécessaire d'encadrer l'utilisation des dispositifs de traitement de données personnelles dans l'entreprise pour que les enjeux qui en découlent soient préservés.

Si la plupart des principes – finalité, licéité, loyauté, proportionnalité, conservation limitée et sécurité des données - posés par le législateur il y a près de quarante ans ont été maintenues voire redessinés, le RGPD et la loi du 20 juin 2018 opère un renversement « complet des logiques antérieures ». La protection des données personnelles des salariés est désormais construite sur une logique de responsabilisation des entreprises et des salariés dont les données sont collectées.

Désormais, la protection des données personnelles est définie de manière concrète et continue par les entreprises chargées d'évaluer les risques d'atteintes aux droits fondamentaux des individus, et de mettre en œuvre des traitements respectueux de ces droits. Les salariés sont également concernés, puisqu'ils interviennent aussi, de manière indirecte, en exerçant leurs droits qui ont été renforcés par le RGPD.

Le rôle de la CNIL a donc du évoluer. Dans un « environnement juridique profondément reconfiguré, elle devient une « autorité de supervision »²⁶⁷, sans pour autant abandonner sa fonction de contrôle, elle aussi largement repensée avec l'attribution de nouveaux pouvoirs.

²⁶⁷ K. FAVRO, « La CNIL, une autorité à "l'âge de la maturité" », *Dalloz IP/IT*, 2018. p.464.

Cependant, l'idée d'une législation de protection à sens unique est largement à relativiser. Pareille conception est battue en brèche par l'affirmation d'objectifs économiques que sous-tend le RGPD. Derrière une volonté de protection se cache en réalité une volonté de faire de l'Europe la nouvelle championne de l'économie de la donnée. Le nouveau droit des données personnelles issu du RGPD a donc une incidence sur les mécanismes de protection des données personnelles des citoyens salariés.

PARTIE 2

L'INCIDENCE DU DROIT DES DONNEES PERSONNELLES SUR LA PROTECTION DES DONNEES PERSONNELLES DES SALARIES

Si le droit des données personnelles est régulièrement avancé comme un droit à vocation protectrice, un regard différent permet de corriger cette vision quelque peu orientée : la liberté de circulation des données personnelles est bien le principe qui gouverne ce droit.

Que dire alors des mécanismes de protection sous l'ère du RGPD ?

Le nouveau droit des données personnelles, induit par l'entrée en vigueur du RGPD, connaît une double influence sur les mécanismes de protection des données personnelles.

D'une part, la consécration du droit des données personnelles met les mécanismes de protection en retrait (Chapitre 1), et d'autre part, la mise en œuvre de ce nouveau droit occasionne une mutation desdits mécanismes (Chapitre 2).

Chapitre I – LA CONSECRATION DU DROIT DES DONNEES PERSONNELLES, SOURCE DE RETRAIT DES MECANISMES DE PROTECTION

La progression du droit des données personnelles n'est pas sans incidence sur la protection de ces dernières. Est observé un recul des mécanismes de protection. Le leitmotiv du RGPD consistant en la promotion de la liberté, la protection revêt le vêtement de l'exception.

La protection excepte ainsi la liberté d'entreprendre de l'employeur (Section 1), tout comme l'objectif de renforcement du Marché intérieur (Section 2) qui sont autant de phénomènes qui appellent analyse.

Section 1 – La protection comme exception à la liberté d'entreprendre de l'employeur

La liberté d'entreprendre de l'employeur trouve des échos significatifs en droit des données personnelles. A cette liberté correspondent deux libertés composites qui animent, grâce au RGPD, la réglementation des données personnelles : la liberté de traitement des données personnelles (§1) et la liberté de sous-traitance (§2).

§1. La liberté de traitement des données personnelles comme composante de la liberté d'entreprendre

Envisagée comme une déclinaison de la liberté d'entreprendre, la liberté de traitement des données personnelles a valeur de principe (A). Ce principe, comme c'est souvent le cas en droit, souffre d'exceptions qu'il convient d'explicitier (B).

A. Le principe de la liberté de traitement des données personnelles

S'il est vrai que la liberté d'entreprendre est absente de la Constitution²⁶⁸, le Conseil constitutionnel en a tout de même fait un principe général ayant valeur constitutionnelle dans sa décision du 16 janvier 1982²⁶⁹.

Présentée comme une composante sinon la conséquence logique de la liberté du commerce et de l'industrie²⁷⁰, cette liberté est autonome et s'entend du droit de créer et d'exercer librement une activité économique dans le domaine de son choix et comme on l'entend.

Cette liberté implique donc la liberté pour toute entreprise de s'administrer et de s'organiser. A ce titre elle comprend d'une part « la liberté de choisir l'objet de l'utilisation de ses moyens de productions, et la liberté d'en choisir la structure »²⁷¹ et d'autre part, « le libre usage du travail et du capital »²⁷².

Puisque l'employeur est en principe libre d'administrer librement son entreprise, la productivité et l'efficacité seront les notions qui présideront à son action lorsqu'il souhaitera mettre en place des dispositifs de traitement des données personnelles. « La liberté de traiter les données personnelles constitue alors un prolongement direct de la liberté de gestion de l'employeur »²⁷³. Et à ce titre, l'employeur est en principe libre de gérer l'entreprise avec les moyens informatiques et les technologies qui s'offrent à lui.

La liberté d'entreprendre de l'employeur est la grande oubliée des contributions d'auteurs travaillistes au sujet des libertés dans l'entreprise. Les droits et libertés fondamentaux des salariés inondent quant à eux les textes de doctrine. La raison peut s'expliquer par l'assimilation faite à tort avec les pouvoirs de l'employeur. Dès que la liberté d'entreprendre entre en contact avec les droits et libertés fondamentaux des salariés alors elle se transforme en faculté d'agir et non en liberté d'agir. Ce paradoxe est souligné par une partie des auteurs qui considèrent qu'effectivement, dans la relation de travail, les libertés se traduisent le plus souvent en droits pour les salariés et en pouvoirs pour l'employeur²⁷⁴.

²⁶⁸ La Constitution espagnole du 6 décembre 1978 garantie quant à elle expressément la liberté d'entreprendre à l'article 38 : « Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación » trad. « La liberté d'entreprise est reconnue dans le cadre de l'économie de marché. Les pouvoirs publics garantissent et protègent son exercice et la défense de la productivité conformément aux exigences de l'économie générale et, s'il y a lieu, de la planification ».

²⁶⁹ Cons.const.16 janv.1982,n°81-132 DC.

²⁷⁰ Cass.soc.,21 juin 2000, n°98-41585 : « L'employeur est responsable de l'organisation, de la gestion, et de la marché générale de l'entreprise, (...), que ce pouvoir de direction découle directement du principe fondamental de la liberté d'entreprendre tel qu'il résulte lui-même du principe de la liberté du commerce et de l'industrie ».

²⁷¹ V. DELVOLVE, « La liberté d'entreprendre », Thèse, Paris II, 2002, p. 212.

²⁷² V.DELVOLVE, « La liberté d'entreprendre », *op.cit.*, p. 244.

²⁷³ N.OCHOA, « Le droit des données personnelles, une police administrative spéciale », Thèse, 2014, p.128.

²⁷⁴ N.OCHOA, *op.,cit.*, p.126.

Cependant il ne faut pas oublier qu'elle constitue le « socle matriciel de l'entreprise »²⁷⁵. Dès lors, au sein de l'entreprise, la liberté d'entreprendre est le principe et sa restriction l'exception. La liberté de traitement primerait alors sur la protection des données personnelles. Cette prévalence de principe est la conséquence directe de la conclusion d'un contrat de travail. Le salarié en se plaçant sous la subordination de son employeur renonce partiellement à son autonomie et accepte implicitement de se soumettre à la liberté d'entreprendre de ce dernier.

Or comme l'objet d'une entreprise est la recherche d'un profit²⁷⁶ et que « l'informatisation confère une force de frappe à l'employeur plus grande »²⁷⁷, les dispositifs de traitement des données personnelles peuvent s'avérer indispensables, sinon nécessaires pour accroître la productivité et donc les profits de l'entreprise. Les dispositifs de traitement des données apparaissent ainsi comme des facteurs de production. En effet, la rationalisation de la procédure de recrutement ou de la gestion RH suppose par définition la mise en œuvre d'un traitement de données personnelles des salariés. Aussi, l'informatisation des entreprises se présente « comme une politique de restructuration de l'appareil économique articulée à de la technologie »²⁷⁸.

Puisque la liberté d'entreprendre constitue le principe et sa restriction l'exception, et que la liberté de traitement des données personnelles est une composante de la liberté d'entreprendre alors la liberté de traitement est le principe et la protection des données personnelles des salariés l'exception.

Malgré la visibilité qui illumine les restrictions en droit positif, la liberté de traitement reste le principe. Sa restriction est alors exceptionnellement limitée. En exprimant la liberté de traitement de manière négative et implicite, l'article L.1121-1 du Code du travail illustre alors parfaitement l'illusion qu'elle est la restriction et non le principe²⁷⁹.

Cette prévalence de principe n'est pas une fatalité puisque si la faillite d'une entreprise est irrémédiable, les atteintes à la protection des données personnelles ne le sont pas. La liberté de traitement des données personnelles, quoiqu'elle constitue le principe, fait l'objet de restrictions.

²⁷⁵ *Ibid.*

²⁷⁶ L'affirmation du Doyen Ripert, « production en vue du profit, recherche du profit illimité, souci constant de ce profit, c'est le but de l'entreprise capitaliste » est d'une consternante réalité.

²⁷⁷ N.OCHOA, *op., cit.*, p.128.

²⁷⁸ *Ibid.*

²⁷⁹ C.trav., art. L.1121-1.

B. Les restrictions à la liberté de traitement de données personnelles

Puisqu'au sein de l'entreprise la liberté de traitement des données personnelles s'analyse comme un pouvoir d'agir, ce n'est qu'en cas de confrontation avec les droits et libertés fondamentaux des salariés qu'elle est restreinte. A défaut de confrontation, l'employeur a « le droit de faire prévaloir sa décision, de trancher, par l'exercice de sa volonté, une situation juridique et d'imposer à autrui la décision prise »²⁸⁰.

Ainsi, l'employeur a la possibilité de prendre une norme ayant une valeur contraignante pour son salarié telle une sanction disciplinaire. L'utilisation de traitements de données personnelles à de telles fins apparaît alors comme une pratique de « contrôle social » faisant référence au pouvoir de cybersurveillance de l'employeur et peut avoir pour finalité l'établissement d'une sanction disciplinaire pouvant aller jusqu'au licenciement pour faute grave.

Plusieurs mécanismes de droit du travail permettent de montrer que la protection des données personnelles est bien l'exception à la liberté de traitement desdites données. S'il n'est pas possible de prétendre à l'exhaustivité, il convient d'en relever quelques-uns.

Tout d'abord, l'instauration d'une présomption de caractère professionnel des messages électroniques opérée par la jurisprudence de la chambre sociale de la Cour de cassation²⁸¹ en est un parfait exemple. En effet, le fleurissement de la protection des correspondances des salariés et, par voie de conséquence de ses données personnelles instaurée par le célèbre arrêt dit « Nikon »²⁸² est en train de périmer. S'il rappelle que le salarié a droit au respect de sa vie privée durant son temps de travail, il s'avère que l'instauration d'une présomption de caractère professionnel des messages qu'il a envoyé depuis l'outil informatique mis à sa disposition pour l'exécution de son travail marque la volonté des juges d'affirmer le principe de la liberté de traitement des données personnelles. L'exception à cette liberté est le fait que le salarié les identifie comme étant personnels dans l'objet du message par exemple²⁸³. Si c'est le cas alors les messages qu'il enverrait seront considérés comme des messages privés auquel l'employeur ne saurait avoir accès. A défaut, l'employeur peut y avoir accès librement hors sa présence²⁸⁴.

²⁸⁰ E. GAILLARD, « Le pouvoir en droit privé », Thèse, *Economica*, 1985.

²⁸¹ Cass. soc., 18 oct. 2006, n°04-48.025.

²⁸² Cass.soc., 2 oct.2001, n°99-42-942.

²⁸³ Cass.soc 30 mai 2007, n°05-43.102.

²⁸⁴ Cass. soc. 4 juillet 2012, n°11-12330.

La même logique s'applique pour les connexions Internet²⁸⁵, à la clé USB personnelle du salarié connecté sur l'ordinateur mis à sa disposition²⁸⁶ et également aux courriels intégrés sur le disque dur de l'ordinateur professionnel du salarié²⁸⁷.

Le rôle du salarié dans la protection de ses données personnelles est donc important puisqu'il doit scrupuleusement identifier ce qu'il souhaite préserver de l'œil de l'employeur²⁸⁸.

Or bien loin d'être parfaite, l'exception de protection est en plus bourrée de failles. Outre la possibilité pratique pour l'employeur de consulter les informations personnelles des salariés en dehors du temps de travail de ces derniers²⁸⁹, l'exception sera bafouée dans le cadre d'une instruction pénale ou d'une décision de justice²⁹⁰. Enfin, le semblant de protection disparaît dans les hypothèses particulièrement vagues de « risques ou évènements particuliers »²⁹¹.

Le régime juridique de la protection des données personnelles des salariés connaît donc bien des limites pratiques. En instaurant une présomption de caractère professionnel, la jurisprudence installe implicitement une présomption de bonne foi de l'employeur dans le respect de la vie privée des salariés. Le salarié se retrouve donc débiteur de la preuve que l'employeur ne l'aurait pas respectée comme par exemple en ouvrant ses fichiers et mails personnels, ce qui relève en pratique d'un véritable parcours du combattant. Par voie de conséquence, la protection des données personnelles passe au second plan même s'il est dans l'intérêt de l'employeur de ne pas s'adonner à ce genre de manipulation au risque de créer un climat de défiance peu propice à la performance et à la productivité des salariés.

Enfin, le régime probatoire et l'interdiction du recours par le salarié à la preuve déloyale illustre bien la position selon laquelle la protection n'est qu'une exception. Or en cas de contentieux prud'homal, l'obtention de preuves par le salarié est particulièrement difficile dans la mesure où la majorité des moyens de preuve se trouvent dans les locaux de l'entreprise et souvent dans l'ordinateur professionnel mis à sa disposition. Si le salarié se fait licencier pour faute grave, ses chances d'en obtenir sont encore plus minimes puisque, souvent assortie d'une

²⁸⁵ Cass.soc., 9 juillet 2008, n°06-42.800.

²⁸⁶ Cass. soc., 12 février 2013, n°11-28.649.

²⁸⁷ Cass. soc., 19 juin 2013, n°12-12.138.

²⁸⁸ Depuis un arrêt du 22 février 2018 de la Cour européenne des droits de l'Homme (v. CEDH, 22 février 2018, requête n°588/13), une vigilance particulière leur est demandée sur l'utilisation des termes employés. En effet, cette dernière a admis qu'un employeur puisse consulter les fichiers d'un salarié, en son absence, s'ils ne sont pas identifiés comme étant privés, et ce même s'il avait utilisé les termes « données personnelles » puisque la charte d'entreprise exigeait expressément cette identification.

²⁸⁹ Bien que cette pratique soit interdite, l'employeur a un accès libre à l'ordinateur. Il pourra alors consulter les informations identifiées comme personnelles mais ne pourra pas en revanche les utiliser en cas de contentieux prud'homal sauf à frauduleusement modifier le nom du fichier.

²⁹⁰ Cass.soc., 10 juin 2008, n°06-16.229.

²⁹¹ Cass.soc., 17 juin 2009, n°08-40274.

mise à pied conservatoire, le salarié se trouve éjecté brutalement de l'entreprise. Son seul recours sera alors la preuve de l'illégalité de l'employeur par l'enregistrement sonore pris durant l'entretien préalable, et ce à condition que l'employeur ne soit pas méfiant et qu'il admet explicitement avoir eu accès aux données personnelles du salarié. En n'étant pas un mode de preuve recevable puisque « clandestin », un déséquilibre naît donc encore une fois en faveur de l'employeur. Il faudrait alors assouplir la traditionnelle rigidité du mode de preuve si elle est nécessaire à l'établissement de la vérité.

Si le régime probatoire n'a pas été mis en place pour servir de « passe-droit » au salarié déloyal et au juge de « statuer sur une vision officiellement tronquée de la réalité »²⁹², il n'en demeure pas moins que la réorganisation du système de preuve ne pourra intervenir que si la protection devient le principe et non l'exception, sans doute au grand dam de l'employeur.

Ainsi, la liberté de traitement des données personnelles est bien le principe et sa restriction l'exception. La protection des données personnelles des salariés apparaît alors en retrait, et dans tous les cas comme un outil d'encadrement de la liberté de traitement. A cet égard, la liberté de sous-traitance suit le même sort.

§2. La liberté de sous-traitance comme composante de la liberté d'entreprendre

La liberté d'entreprendre de l'employeur implique également la liberté de recourir à la sous-traitance, source de nombreux avantages²⁹³. Si la primauté de la liberté d'entreprendre est clairement exprimée par l'aménagement de la responsabilité de ces derniers (B), le RGPD conscient du recours croissant aux sous-traitances a consacré la notion de coresponsabilité permettant de souligner que si la protection est en retrait, elle n'est cependant pas oubliée (A).

A. La consécration d'une responsabilité conjointe

Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte du responsable de traitement²⁹⁴. Tous deux sont donc amenés à traiter des

²⁹² J.MOULY ET J.SAVATIER, « Droit disciplinaire – Fautes disciplinaires », *RDT*, 2019.

²⁹³ Le recours à la sous-traitance présente un avantage indéniable pour l'employeur puisqu'elle permet de réduire les coûts tout en permettant la réalisation d'une tâche spécifique confiée à un service compétent. Le développement informatique et les compétences techniques qu'il implique ont eu raison des entreprises, qui dans leur objectif de performance et de rentabilité, ont dû recourir à des prestataires pour externaliser leurs services comme notamment la paie, ou la sécurité du réseau informatique.

²⁹⁴ Règl.n°(UE) 2016/679, *op.,cit.*,art 4.8.

données personnelles à la seule différence que le sous-traitant traite des données non pas en autonomie mais pour le compte du responsable de traitement. Dès lors, en décidant des finalités et des moyens du traitement²⁹⁵, c'est le responsable qui engage sa responsabilité en cas de non-conformité. L'intérêt de la distinction entre les deux qualifications porte donc sur la répartition de la responsabilité de chacun.

Toutefois l'intérêt de la distinction, traditionnellement utilisée en matière de responsabilité, s'édulcore quelque peu. En effet le niveau de responsabilité des sous-traitants a été significativement renforcé. Contrairement à l'ancienne législation, ils sont désormais responsables du traitement des données confié dans le contrat de sous-traitance. Ainsi, ils sont tenus de documenter leurs conformités (respect des obligations en matière d'accountability) sur d'autres questions que celles relatives à la sécurisation technique des données²⁹⁶. Ce niveau d'exigence se répercute également dans les chaînes de sous-traitance.

Cependant, il se peut qu'en pratique, le responsable de traitement dispose d'une autonomie assez importante. La distinction entre les deux s'avère alors assez nébuleuse. Cette autonomie se traduit par la détermination des finalités et des moyens du traitement de données personnelles. L'intégralité des finalités et des moyens n'est donc plus exclusivement faite par le responsable de traitement mais est ici partagée avec le sous-traitant. Nait donc, à l'image du co-emploi, une coresponsabilité dans le traitement des données personnelles²⁹⁷. Le sous-traitant devient ainsi responsable de traitement au même titre que son cocontractant.

Outre l'obligation pour le responsable de traitement de choisir des sous-traitants présentant des garanties suffisantes²⁹⁸, le contrat de sous-traitance doit clairement préciser leurs responsabilités et le rôle respectif de chacun voire prévoir un partage de responsabilité sur certaines catégories de traitement, étant toujours précisé qu'une requalification peut s'opérer.

De même le contrat, qui doit être mis à disposition des salariés concernés pour qu'ils puissent connaître la possibilité d'exercer leurs droits auprès de l'un ou l'autre, doit faire clairement ressortir que les données ne pourront être traitées par le sous-traitant que sur

²⁹⁵ Règl.n°(UE) 2016/679, *op.*, *cit.*, art 4.7.

²⁹⁶ Sous l'ancienne législation, les sous-traitants n'étaient pas responsables des manipulations qu'il opérait sur les données confiées par le responsable de traitement à l'exception des questions de sécurisation des données.

²⁹⁷ Règl.n°(UE) 2016/679, *op.*, *cit.*, art 26.

²⁹⁸ Les sous-traitants ne peuvent par ailleurs eux-mêmes recourir à des sous-traitants sans l'accord du responsable de traitement.

instructions du responsable de traitement, sauf obligation légale²⁹⁹. A défaut, il s'expose à un risque de requalification de sa qualité de sous-traitant à responsable de traitement³⁰⁰.

La CNIL ou le juge ne sont en effet pas liés par la qualification que les parties ont donnée au contrat de sous-traitance. Derrière un faux contrat de sous-traitance peut en réalité se cacher une dualité de responsables de traitement. C'est donc en tenant compte des conditions réelles d'exécution du contrat de sous-traitance que la CNIL ou le juge détermineront la réalité dudit contrat. Pour y parvenir, ces derniers feront une appréciation *in concreto* de chaque dispositif de traitement et ce en vertu du traditionnel et imprescriptible faisceau d'indices³⁰¹. En fonction de cette appréciation, le sous-traitant pourra alors revêtir la qualification de responsable de traitement uniquement pour certaines catégories de traitements et non pour toutes³⁰².

Le sous-traitant pourra en conséquence voir sa responsabilité engagée de manière autonome s'il n'a pas respecté les obligations prévues par le RGPD, ou s'il a agi en dehors ou contrairement aux instructions licites du responsable de traitement³⁰³. A contrario, si dans la réalité, il participe au même titre que le responsable à la détermination des moyens et des finalités du traitement, il revêtira la qualité de coresponsable et pourra voir sa responsabilité engagée en cas d'atteintes aux données personnelles des salariés. Il est ici fait recours aux mécanismes de droit civils puisqu'étant coresponsables, en cas de défaillance à la réglementation en matière de données personnelles, le salarié pourra exercer ses droits à l'encontre de l'un ou de l'autre. Chacun d'eux sera alors tenu responsable du dommage dans sa totalité. La volonté de protéger les données personnelles des salariés à l'égard du recours au contrat de sous-traitance transparait puisqu'il s'agit d'une responsabilité *in solidum*³⁰⁴, ce qui permet de garantir au salarié une réparation effective³⁰⁵ et éviter « toute dilution de responsabilité »³⁰⁶. Le responsable de traitement ayant réparé totalement le dommage subi sera

²⁹⁹ Toute la question sera alors de savoir ce qu'on entend par obligation légale. Encore un beau champ à contentieux qui se prépare.

³⁰⁰ C.CASTETS-RENARD, « La protection des données personnelles dans les relations internes à l'Union européenne », *Dr.soc.* 2018 (actualisation : Mai 2019).

³⁰¹ Sont pris en compte, le niveau d'instruction donné par le client aux prestataires, le degré de contrôle de l'exécution de la prestation du prestataire par le client responsable de traitement, la valeur ajoutée fournie par les prestataires sur le traitement des données des clients ainsi que le degré de transparence sur le recours à un prestataire.

³⁰² Par exemple, il pourra être considéré comme co-responsable de traitement pour la gestion des services paie qui lui ont été externalisés mais gardera sa qualité de sous-traitant en ce qui concerne les dispositifs de carrières des salariés.

³⁰³ Règl.n°(UE) 2016/679, *op.,cit.*, art 82.2.

³⁰⁴ Règl.n°(UE) 2016/679, *op., cit.*, art 82.4.

³⁰⁵ C.CASTETS-RENARD, *art.,préc.*

³⁰⁶ L.CLUZEL-METAYER ET E.DEBAETS, *art., préc.*, p.1101.

alors en droit de réclamer auprès de l'autre la part de la réparation correspondant à sa part de responsabilité dans le dommage³⁰⁷. Une action récursoire est donc possible.

Le principe reste néanmoins la liberté de recourir à la sous-traitance et ce n'est que par exception qu'apparaît la volonté de protéger le citoyen-salarié contre les fausses sous-traitances ou celles peu fiables. C'est donc au travers l'extension de la responsabilité autonome du sous-traitant et la consécration d'une éventuelle coresponsabilité avec le responsable de traitement que la volonté de protection transparait. Néanmoins, si le RGPD a instauré un régime de responsabilité civile nouveau pour le sous-traitant, la responsabilité se trouve ménagée, ce qui démontre encore une fois un retrait de la protection pour servir la liberté d'entreprendre de l'employeur.

B. L'affirmation d'une responsabilité ménagée

Si le RGPD met à la charge des responsables de traitement et des sous-traitants des obligations plus nombreuses, le respect de celles-ci leur permet de ménager plus facilement leur responsabilité contrairement aux législations précédentes. Le vertige que peut provoquer la liste des nouvelles obligations pour ces derniers est donc mesuré.

Même si le texte est muet sur la nature de leurs obligations, il est possible d'affirmer que d'une obligation de résultat, ces derniers sont désormais débiteurs d'une obligation de moyens renforcée³⁰⁸.

D'origine doctrinale³⁰⁹, la distinction entre ces deux types d'obligations revêt un intérêt non négligeable sur le régime probatoire notamment sur la charge de la preuve. Si l'obligation de résultat implique le constat d'un manquement à une obligation, l'obligation de moyens oblige le salarié lésé à prouver la faute de son employeur. En effet, l'obligation de moyens engage l'employeur à mettre en œuvre tous les moyens en sa possession pour respecter les nouvelles prescriptions du RGPD. Le résultat d'une protection totale et exempte de toutes atteintes ne peut cependant être affirmé avec certitude. A l'inverse, l'obligation de résultat engage l'employeur quant au résultat à atteindre. Sa défaillance n'est pas permise. Il ne pourra s'exonérer de sa responsabilité qu'en prouvant que la défaillance est due à une cause étrangère et extérieure. La notion de force majeure prend alors vie.

³⁰⁷ Règl.n°(UE) 2016/679 du parlement européen et du Conseil, 27 avr 2016, *op., cit.*, art 82.5.

³⁰⁸ G.DESGENS-PASANAU, *art., préc.*, p.8.

³⁰⁹ R.DEMOGUE, « Traité des obligations en général », 1923, p. 599.

Ainsi en passant d'une obligation de résultat à une obligation de moyens renforcée ou à une « obligation de résultat atténuée »³¹⁰, le RGPD modifie radicalement la donne.

Auparavant, la loi « Informatique et libertés » était indifférente aux diligences que le responsable de traitement devait entreprendre pour protéger les données personnelles des salariés. Il suffisait qu'un manquement à une obligation soit constaté pour que la CNIL se saisisse et prononce une sanction.

Le RGPD met donc en avant la prééminence accordée à la liberté d'entreprendre de l'employeur puisque désormais si ce dernier ou son sous-traitant engagent une réelle démarche de mise en conformité à la réglementation, les risques de sanction sont faibles. Ainsi le passage d'une démarche de contrôle a priori à une démarche de responsabilisation a instauré une présomption de conformité à la réglementation. La bonne foi de l'employeur occupe alors une place importante et ce même si la charge de la preuve de la conformité appartient aux responsables de traitement et aux sous-traitants.

Dès lors, malgré les discours tendant à affirmer que le RGPD a instauré un régime de responsabilité contraignant et fastidieux, les responsables de traitement et les sous-traitants « sont en réalité plus protégés qu'ils ne l'étaient auparavant »³¹¹ puisqu'ils sont invités à agir « dans la mesure du possible »³¹². Si pour les grandes entreprises, cet aménagement de responsabilité est la cerise sur le gâteau, elle est en revanche souhaitable pour les TPE/PME. En effet, il ne faut pas décourager ces entreprises qui face à la liste vertigineuse d'obligations leur incombant renoncent à l'action en considérant qu'il s'agit d'un poste de charges supplémentaire dépourvu de plus-value³¹³.

En définitive, si le RGPD prône une extension de responsabilité donnant l'illusion de faire la protection des données le principe, l'aménagement de la responsabilité qu'il offre au responsable de traitement et aux sous-traitants permet d'affirmer que la protection n'est qu'une exception à la liberté d'entreprendre de l'employeur. La liberté d'entreprendre n'est pas la seule concernée. En effet, derrière les belles paroles tendant à faire du RGPD un outil de protection des données personnelles, se cache en réalité un objectif de renforcement du Marché intérieur.

³¹⁰ P.LE TOURNEAU, « Inexécution d'une obligation contractuelle professionnelle et normes de référence », *DRC*, 2018-2019.

³¹¹ G.DESGENS-PASANAU, *op.cit.*, p.8.

³¹² L.CLUZEL-METAYER ET E.DEBAETS, *art., préc.*

³¹³ S.MILLET, « La protection des données personnelles en chantier : le RGPD vu sous l'angle des données RH », *Cabinet ELLIPSE Avocat*, 2018.

Section 2 – La protection comme exception à l’objectif de renforcement du Marché intérieur

Malgré l’objectif de protection inclus au sein même de l’acronyme du RGPD, il s’avère que l’objectif de protection n’est qu’une parade à des objectifs d’ordre économique. Réformer la protection des données personnelles est apparu nécessaire puisque cette dernière était perçue comme une entrave à la compétitivité des entreprises (§1) et se prêtait mal à l’internationalisation des flux transfrontaliers (§2) indispensable au renforcement du Marché intérieur.

§1. La protection comme entrave à la compétitivité des entreprises

Dans sa quête incessante de renforcement du Marché intérieur, l’Union européenne appelle de ses vœux à une liberté, source d’épanouissement pour les entreprises. La protection des données personnelles y constitue à l’évidence un obstacle. Partant, l’uniformisation de la législation en la matière s’avère être impondérable à la compétitivité espérée (A). La réalité dépeint toutefois un autre tableau : celui d’une uniformisation partielle (B).

A. Une uniformisation nécessaire pour favoriser la concurrence

Malgré la reconnaissance de la protection des données personnelles comme droit fondamental³¹⁴ et un rappel de bonne intention³¹⁵, le RGPD dévoile très rapidement son ambition. L’objet du RGPD, c’est-à-dire sa raison d’être, est de « contribuer à la réalisation d’un espace de liberté, de sécurité et de justice et d’une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu’au bien-être des personnes physiques »³¹⁶. Le renforcement du Marché intérieur par la construction d’un marché unique numérique³¹⁷ serait donc l’objectif prioritaire.

La logique du Marché intérieur est donc fortement présente. Or une réglementation trop protectrice des données personnelles constituerait un frein au renforcement du Marché

³¹⁴ Règl.n°(UE) 2016/679, *op.,cit.*, considérant 1.

³¹⁵ En passant de l’expression « l’informatique doit être au service des citoyens » au principe figurant au considérant 4 selon lequel « le traitement des données personnelles devrait être conçu pour servir l’humanité », le législateur européen rappelle a priori la primauté de la protection des données personnelles.

³¹⁶ Règl.n°(UE) 2016/679, *op.,cit.*, considérant 2.

³¹⁷ A.STROWEL, « Quelles protections des données personnelles en Europe ? », *Larcier*, 2015, p.13.

intérieur. Autrement dit, la protection des données personnelles entraverait le Marché intérieur. Dès lors, le renforcement du Marché intérieur reposerait principalement sur « la levée des restrictions injustifiées à la libre circulation des données »³¹⁸.

C'est pourquoi le RGPD a diminué les charges administratives des entreprises en supprimant les mécanismes de formalités préalables qui représentaient un coût très élevé et qui pouvaient être considérés comme la cause du dysfonctionnement du Marché intérieur³¹⁹.

L'uniformisation de la réglementation applicable en matière de traitement de données personnelles est alors apparue comme une nécessité. A la volonté d'harmonisation opérée par la directive de 1995, a succédé la volonté d'uniformisation des législations des Etats membres afin de remettre les acteurs européens et internationaux à égalité de concurrence. Désormais les entreprises définissent par elles-mêmes la politique de protection des données personnelles. L'objectif de cet assouplissement des mécanismes de protection est donc de renforcer la compétitivité³²⁰ des entreprises européennes face aux acteurs américains dont la confrontation des visions est au cœur d'un enjeu de domination du marché économique.

Cette uniformisation est une chance pour le développement économique des entreprises européennes. En permettant à l'Union européenne de disposer d'un outil unifié, l'adoption du RGPD permet aux entreprises de peser plus lourdement dans le marché de l'économie de la donnée. Si la préoccupation de créer une économie de la donnée devenue « une ressource essentielle pour la croissance économique, la création d'emploi et le progrès social »³²¹ n'est pas nouvelle, la volonté de peser sur la scène internationale est clairement affirmée.

En effet, le traitement de données personnelles contribue au « pouvoir de marché »³²² d'une entreprise. Puisque les données sont des denrées commerciales, si les activités commerciales des entreprises européennes se révèlent entravées par de trop nombreuses règles de protection, il est à craindre que le développement de l'économie numérique dans un monde concurrentiel exacerbé ne puisse jamais être atteint. Le sacro-saint marché unique ne doit donc

³¹⁸ CE, 8 février 2017, 10ème - 9ème Chambres réunies, n° 393714, p.9.

³¹⁹ J-L.SAURON, « Le RGPD : outil ou entrave de la société d'information ? », *Dalloz IP/IT*, 2016 p.17

« Le RGPD : outil ou entrave de la société d'information ? », *Dalloz*, « Le RGPD », 2018, p.75.

³²⁰ G.DESGENS-PASANAU, *art.préc.*, p.6 ; La compétitivité d'une entreprise est sa capacité à faire face à la concurrence d'un marché.

³²¹ Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et 1062 au comité des régions, Com (2017) 9 final, « Créer une économie européenne fondée sur les données », Bruxelles, 2017, p. 2.

³²² C.CASTETS-RENARD, « Quelles protections des données personnelles en Europe ? », Larcier, 2015, p.28. « Le pouvoir de marché d'une entreprise définit sa latitude à fixer les prix de vente sur un marché donné au-dessus de ses coûts de production sans tenir compte de ses concurrents. Cette détermination comprend plusieurs éléments dont l'analyse de concurrents, la disponibilité de produits substituables ou encore l'existence de barrière à l'entrée ».

pas sortir affaibli par une législation protectrice des données personnelles. Dès lors, la protection se trouve circonscrite à son versant économique.

Si le RGPD doit être analysé comme un outil permettant de renforcer la compétitivité des entreprises, le risque que la protection des données personnelles soit bradée est important. La domination d'un marché économique fondé sur la donnée est alors le principe et la protection l'exception.

En définitive, affirmer que l'adoption du RGPD avait pour objectif d'assurer la protection des données personnelles aboutit à une vision tronquée du RGPD. En effet, le droit positif met clairement en exergue la volonté d'assurer la compétitivité des entreprises. Le citoyen n'est pas dupe et ne se fera pas endormir par les belles paroles promouvant une protection renforcée alors que des arguments économiques lui sont exposés. La protection des données personnelles est alors instrumentalisée au profit du renforcement du Marché intérieur.

Alors que la volonté du RGPD était de créer un même droit sur tout le continent européen et d'être valable uniformément dans tous les Etats-membres, il s'avère que cet objectif d'uniformisation n'est pas complet et est partiellement atteint.

B. Une uniformisation partielle atteinte

Le choix d'adopter un règlement européen sur la protection des données personnelles n'est pas anodin. En effet, un règlement européen se distingue d'une directive européenne. Cette dernière lie les Etats-membres seulement quant au résultat à atteindre. Elle leur laisse alors le « choix de la forme et des moyens à adopter dans leur ordre juridique interne pour atteindre l'objectif »³²³. Un règlement quant à lui implique une application directe et donc en principe une législation unique sur l'ensemble du territoire de l'Union européenne. L'objectif est alors de « réduire la fragmentation juridique entre les Etats-membres »³²⁴. Si une directive ne réduit pas l'autonomie des Etats, le règlement met quant à lui normalement fin aux spécificités nationales.

Cependant l'objectif « one law one continent »³²⁵ sans possibilité d'adaptation n'est pas totalement atteint. En effet le RGPD comporte cinquante-six possibilités d'adaptation dont

³²³ G.DESGENS-PASANAU, *art., préc.*, p.7.

³²⁴ G.DESGENS-PASANAU, *ibid.*

³²⁵ E.BRUNET, « Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation global », *Dalloz IP/IT*, 2016.

l'Etat membre peut ou non faire usage. Des mesures spécifiques sont donc attendues. Le traitement opéré dans le cadre des relations de travail n'y échappe pas³²⁶. Dès lors au sein même des entreprises, des disparités sont à prévoir quant à la politique de protection des données des salariés qu'elles entendent mettre en œuvre. Le souhait d'éviter « le forum shopping »³²⁷ n'était donc qu'une utopie puisque les Etats membres et les entreprises pourront se saisir des marges de manœuvre offertes. Des disparités entre les juridictions et dans l'efficacité des mécanismes de protection vont se créer alors même que l'objectif initial était de mettre fin au principal reproche de la directive de 1995 tendant à l'absence l'uniformisation des règles.

Si l'objectif du RGPD est de créer « des champions européens sur la scène internationale », et de rendre l'Union européenne « attractive pour les entreprises souhaitant offrir leurs services sur le gigantesque marché européen »³²⁸, il se peut que le RGPD crée des écarts de compétitivité au sein même de l'Union européenne entre les Etats-membres. Le risque d'une « carte de vingt-huit législations et jurisprudences appliquées »³²⁹ est donc à craindre. Des manœuvres stratégiques sont attendues sur le choix de l'Etat membre qui permettra à l'entreprise d'être la plus compétitive et où la « protection des données personnelles sera la mieux contrebalancée avec les objectifs économiques »³³⁰. La reprise en main par le législateur européen des prérogatives jusqu'alors confiées aux législateurs nationaux est encore loin de voir le jour de manière uniforme et « l'objectif politique de limiter les décisions de certaines autorités nationales de protection des données considérées comme trop « zélées » »³³¹ n'est pas près de se réaliser.

Ainsi au regard de l'importance des enjeux, il apparaît plus sage que les entreprises s'approprient l'outil RGPD pour que ce dernier devienne un outil de compétitivité en soi, un « argument marketing à part entière »³³² et par là créer de la compétitivité dans la protection des données elle-même. Rien de tel qu'une entreprise privilégiant les individus en leur assurant un niveau de protection élevé des données. L'objectif sera donc d'adopter une politique de protection pour éviter que les foudres médiatiques et citoyennes ne s'abattent sur l'entreprise

³²⁶ Règl.n°(UE) 2016/679, op., cit., art 88.

³²⁷ Le forum shopping fait référence à une pratique de droit international privé consistant à saisir la juridiction la plus susceptible de donner raisons à ses propres intérêts. Appliqué à l'économie numérique, cette notion fait référence au lieu d'implantation d'une entreprise dans l'Etat où les règles sont plus favorables.

³²⁸ E.BRUNET, *art., préc.*, p.42.

³²⁹ J-L.SAURON, *art., préc.*, p.81.

³³⁰ J-L.SAURON, *ibid.*

³³¹ G.DESGENS-PASANAU, *art., préc.*, p.7.

³³² J-L.SAURON, *art., préc.*, p.80.

et nuisent à sa réputation. L'exemple de Facebook en est un marqueur flagrant. La protection est alors marginalisée et encore une fois instrumentalisée derrière « un discours marketing éthique vantant le respect de la législation sur les données personnelles »³³³.

Puisque le marché européen est constitué d'un peu plus de 500 millions de personnes, il représente des intérêts économiques majeurs au plan international. La volonté d'uniformiser les règles applicables au sein de l'Union européenne sans garantir leur applicabilité à l'ensemble des acteurs y exerçant une activité aurait abouti à produire l'effet inverse recherché à savoir « créer un déséquilibre concurrentiel en défaveurs des entreprises européennes »³³⁴. C'est ainsi, toujours dans l'objectif caché de renforcer le marché intérieur et dans l'objectif apparent de protection des données, qu'il est apparu nécessaire de construire un corpus de règles applicables pour adapter la législation aux réalités économiques, notamment au développement des flux transfrontaliers.

§2. La protection à l'épreuve de l'internationalisation des flux transfrontaliers

Le développement des flux transfrontaliers a exigé l'évolution de la délimitation territoriale des règles européennes relatives à la protection des données personnelles. Le champ d'application territorial a donc été étendu d'une part en raison de la déterritorialisation (A), et d'autre part en raison des transferts de données personnelles hors Union européenne (B).

A. Une extension du champ d'application territorial en raison de la déterritorialisation

Aujourd'hui les critères d'application de la réglementation relative à la protection des données personnelles, c'est-à-dire l'exigence de la présence d'un établissement ou de moyens sur le territoire d'un Etat-membre prévue par la directive de 1995³³⁵, ne sont plus apparus suffisants face à un monde toujours plus dématérialisé et déterritorialisé.

Le RGPD a donc repris les critères traditionnels en élargissant leur portée mais est également allé plus loin en consacrant une nouvelle règle d'applicabilité. Deux critères sont pris en compte : le critère de territorialité de l'entreprise et le critère de territorialité des activités de traitement.

³³³ C.CASTETS-RENARD, *art., préc.*, p.29.

³³⁴ E.BRUNET, *art., préc.*, p.43.

³³⁵ Dir. 95/46/CE, *op., cit.*, art 4.1.

Le premier critère concerne l'entreprise ou son sous-traitant qui sont établis au sein de l'Union européenne. Le RGPD s'applique alors aux « traitements de données personnelles effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'UE »³³⁶. Derrière ces mots, il est à noter que le lieu de traitement n'a plus aucune incidence. Il ne sera donc désormais plus possible d'échapper « aux griffes de la réglementation RGPD en faisant héberger son système de traitement loin des frontières européennes »³³⁷. En effet, le critère qui l'emporte est celui de « l'établissement » qui « suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable »³³⁸, soit un joli champ à contentieux.

Le deuxième critère concerne l'entreprise ou son sous-traitant qui n'est pas établi au sein de l'Union européenne mais qui y déploie une activité conduisant à la collecte et au traitement de données personnelles. Plus exactement toutes les activités de traitement liées à l'offre de biens ou de services, avec ou sans paiement³³⁹, mais également le suivi de comportements³⁴⁰ repérés au sein de l'Union européenne seront soumis au RGPD dès lors qu'ils ciblent des personnes situées sur le territoire de l'Union européenne³⁴¹. L'application extraterritoriale du RGPD est donc consacré par l'article 3§2 en exigeant le critère des activités dirigées vers l'Union européenne indépendamment d'une présence physique préalable de l'entreprise sur le territoire de l'Union. Sont visées ici les entreprises internationales de e-commerce dès lors que leurs activités ciblent des personnes situées sur le territoire européen. Une analyse fonctionnelle est donc opérée fondée sur l'appréciation de l'activité réelle sur le territoire européen³⁴².

Il est à noter que si le champ d'application de la directive de 1995 a été étendu à des activités menées hors Union européenne par la jurisprudence de la Cour de Justice européenne

³³⁶ Règl.n°(UE) 2016/679, *op., cit.*, art 3.

³³⁷ R.PERRY, « La délimitation territoriale du RGPD : le champ d'application et les transferts de données hors de l'Union européenne », *Daloz IP/IT*, 2016, p. 581.

³³⁸ Règl.n°(UE) 2016/679, *op., cit.*, art 22.

³³⁹ Règl.n°(UE) 2016/679, *op., cit.*, art 3.2 Le RGPD précise en son considérant 23 que des facteurs tels que « l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs Etats membres, avec la possibilité de commander des biens ou des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union » peuvent être des indices permettant de déterminer la volonté du responsable d'offrir ses biens ou servir à des personnes se trouvant sur le territoire de l'Union européenne.

³⁴⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 3.3. Le RGPD précise en son considérant 24 que sont concernées entre autres, les techniques de profilage d'une personne physique permettant « notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ».

³⁴¹ Règl.n°(UE) 2016/679, *op., cit.*, art 3.2.

³⁴² P.CADIO ET T.LIVENNAIS, « Photographie du champ territorial du règlement données personnelles : de nouveaux opérateurs concernés ? », *Daloz IP/IT*, 2016.

dans l'arrêt dit « Google Spain » du 13 mai 2014³⁴³, la Cour exigeait une présence physique de l'entreprise sur le sol de l'Union européenne, ce que le RGPD ne fait pas. S'il a pris acte de cette jurisprudence, le RGPD va donc encore plus loin puisqu'aucune présence physique de l'entreprise établie sur le territoire de l'UE n'est imposée.

Cette extension du champ d'application du RGPD est d'une importance certaine puisque « les arguties liées à la territorialité, déployées par force de conviction par les armées d'avocats n'auront qu'un intérêt théâtral à l'avenir »³⁴⁴.

La volonté de renforcer le Marché intérieur face aux nouveaux concurrents virtuels ou ceux établis en dehors de l'Union européennes est donc clairement affirmé. Le RGPD se voit ainsi applicable sur la scène internationale pour faire face à la mondialisation et promouvoir les principes européens.

En définitive, il est possible d'affirmer que le droit des données personnelles n'est pas exclusif de l'intérêt des salariés. Il s'est avéré nécessaire d'adapter la protection au quotidien des entreprises et à leurs impératifs économiques et sociaux afin de favoriser le renforcement du Marché intérieur.

Cependant, dans certains cas, les entreprises situées hors Union européenne ne relèveront pas des critères d'applicabilité du RGPD mais recevront des données personnelles de citoyens-salariés. Dès lors, pour mieux tenir compte du numérique, le champ d'application des transferts hors Union européenne a dû être étendu.

B. Une extension du champ d'application en raison des transferts hors Union européenne

Appliquée à la relation de travail, la question des transferts de données personnelles d'une entreprise à une autre revêt une importance particulière en raison de l'augmentation du nombre de restructurations d'entreprises. Si les transferts de données personnelles sont libres dans les pays membres de l'Union européenne, hors Union européenne la procédure de

³⁴³ CJUE, 13 mai 2014, Google Spain, aff. C-131/12, JurisData n°2014-009597. La Cour a considéré que la directive de 1995 était territorialement applicable bien que le traitement soit effectué par Google Inc., dont le siège social est établi aux Etats-Unis tandis que l'activité de Google Spain, établissement ayant son siège à Madrid, se limitait à la promotion de ventes d'espaces publicitaires. Même si le traitement n'est pas réalisé par l'établissement espagnol, le fait qu'il soit réalisé dans le cadre de ses activités, suffit pour que le droit européen s'applique.

³⁴⁴ M.REES, sur son blog : « Le RGPD expliqué ligne par ligne », 2018.

transfert est renforcée, en raison de la diversité et de l'efficacité variable des dispositifs de protections étrangers.

Le principe reste celui de l'interdiction des transferts³⁴⁵ sauf si l'Etat tiers assure un niveau de protection suffisant, lequel est formellement reconnu par une « décision d'adéquation » adoptée par la Commission européennes³⁴⁶. L'objet de ces décisions est de vérifier que le niveau de protection des données personnelles des pays tiers une fois le transfert effectué « assure au citoyen une protection équivalente à celle que leur offre la réglementation européenne »³⁴⁷. Dans une pareille hypothèse, ce « transfert ne nécessite pas d'autorisation spécifique ». Or, à ce jour, peu de pays bénéficient de cette décision d'adéquation³⁴⁸.

Les dérogations à ce principe d'interdiction sont maintenues mais le RGPD consacre « le recours alternatif et même en cascade »³⁴⁹ du transfert à d'autres possibilités.

En effet, à défaut de décision d'adéquation, une société française ne pourra transférer des données personnelles que si le pays tiers a prévu des « garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives »³⁵⁰. Ces garanties appropriées sont de plusieurs sortes, les deux principales étant les clauses contractuelles types émanant de la Commission³⁵¹ ou alors les règles internes contraignantes communément appelées les « Binding Corporate Rules » dites « BCR »³⁵². C'est une innovation du RGPD puisque les anciennes législations n'y faisaient pas référence. Le principal intérêt du recours aux BCR est son caractère contraignant et sa grille d'évaluation en termes de contenu, d'opposabilité des règles et d'effectivité de leur application³⁵³. Cependant ces BCR ne s'appliquent qu'aux transferts au sein d'un même groupe, la notion de groupe s'entendant au-delà de la notion de contrôle capitalistique³⁵⁴.

³⁴⁵ Règl.n°(UE) 2016/679, *op., cit.*, art 44.

³⁴⁶ Règl.n°(UE) 2016/679, *op., cit.*, art 45.

³⁴⁷ F. JAULT-SESEKE ET C. ZOLYNSKI, « Le règlement 2016/679/UE relatif aux données personnelles, *ADIP*, 2016, p. 1877.

³⁴⁸ Il s'agit des pays membres de l'Association européenne de libre-échange de l'Espace économique européen à savoir la Norvège, l'Islande, et le Liechtenstein, ainsi que les sept pays et territoires suivants : Suisse, Canada, Argentine, Ile de Man, Iles Anglo-Normande, Nouvelle-Zélande et Israel.

³⁴⁹ R.PERRAY, *art., préc.*, p.59.

³⁵⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 46.

³⁵¹ Règl.n°(UE) 2016/679, *op., cit.*, art 46.2.

³⁵² Règl.n°(UE) 2016/679, *op., cit.*, art 47.

³⁵³ F.NAFTALSKI, « L'impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT*, 2016, p.340.

³⁵⁴ Règl.n°(UE) 2016/679, *op., cit.*, considérant 37 : « Un groupe d'entreprises devrait couvrir une entreprise qui exerce le contrôle et ses entreprises contrôlées, la première devant être celle qui peut exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel. Une entreprise qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées devrait être considérée comme formant avec ces dernières un groupe

Cependant les BCR ne sont pas seuls puisque le RGPD enrichit les mécanismes encadrant les transferts hors Union européenne. Trois nouvelles garanties sont prévues : les clauses types de protection adoptées par la CNIL et approuvées par la Commission³⁵⁵, les codes de conduites³⁵⁶ et les mécanismes de certification³⁵⁷ tous deux assortis de l'engagement contraignant et exécutoire pris par l'entreprise ou son sous-traitant d'appliquer des garanties en ce qui concerne les droits et libertés fondamentaux des personnes. Ces garanties permettront alors à la société de transférer les données sans autorisation de la CNIL. Des clauses ad hoc pourront être adoptées par les parties au transfert mais dans ce cas l'autorisation de la CNIL est indispensable³⁵⁸.

Puisque le salarié ne dispose pas d'une autonomie en raison de sa subordination envers l'employeur, il est inutile de considérer que le transfert est possible en cas de consentement de ce dernier³⁵⁹, mais a contrario il devient possible s'il est nécessaire à l'exécution du contrat de travail³⁶⁰.

Outre le mécanisme de Privacy Shield³⁶¹, il convient de relever une particularité concernant le transfert de données personnelles avec les Etats-Unis : la procédure de « Discovery ». Cette procédure est « la phase d'investigation et d'instruction préalable au procès civil et commercial qui est essentielle pour toute action en justice aux Etats-Unis. Or, les demandes de communication qui sont faites à cette occasion peuvent concerner d'innombrables données personnelles des salariés comme notamment les courriers électroniques. Au cours des auditions qu'elle a menées, la CNIL a constaté la multiplication des cas de communication de données de la France vers les autorités judiciaires américaines dans le cadre de ces procédures de Discovery »³⁶². Assurément cette procédure peut altérer la protection des données personnelles des salariés, d'autant plus avec l'apparition relativement

d'entreprises ». Dès lors le groupe couvre une entreprise qui exerce une influence dominante sur les autres entreprises du fait par exemple de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer des règles relatives à la protection des données personnelles.

³⁵⁵ Règl.n°(UE) 2016/679, *op., cit.*, art 46.2 d).

³⁵⁶ Règl.n°(UE) 2016/679, *op., cit.*, art 46.2 e).

³⁵⁷ Règl.n°(UE) 2016/679, *op., cit.*, art 46.2 f).

³⁵⁸ F.NAFTALSKI, *art.préc.*, p.24.

³⁵⁹ Règl.n°(UE) 2016/679, *op., cit.*, art 49.1 a).

³⁶⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 49.1 b).

³⁶¹ Suite à la censure des Safe Harbor par la Cour de Justice de l'Union européenne le 6 octobre 2015 (v. CJUE 6 oct.2015, aff. C-362/14, Schrems c/Data Protection Commissioner), c'est sur le mécanisme de Privacy Shield que repose le transfert de données puisqu'il reconnaît l'existence de garanties suffisantes aux Etats-Unis. Sauf exceptions, les entités certifiées Privacy Shield s'engageront à respecter : le principe de notification recouvrant le principe d'information, d'intégrité des données et de limitation des finalités, le principe de choix, de sécurité et le principe d'accès aux données ne pouvant être restreints que dans des cas exceptionnels.

³⁶² <https://www.cnil.fr/fr/quel-cadre-juridique-pour-les-procedures-de-discovery-0>

récente de la procédure de « e-discovery »³⁶³. C'est d'ailleurs en raison de la multiplication de ces deux procédures que la CNIL a publié une recommandation en 2009³⁶⁴.

Ainsi, la reconnaissance par le RGPD de nouveaux mécanismes favorisant les transferts internationaux de données personnelles doit être saluée³⁶⁵ puisque ces derniers permettent le renforcement du marché intérieur tout en assurant un niveau de protection adéquat. Le subtil équilibre a priori infranchissable a été réussi ce qui permet de rendre crédible et attractif le marché européen.

En définitive, il semble que « les règles relatives aux transferts ont été conçues comme le prolongement naturel de celles concernant le champ d'application territorial »³⁶⁶.

CONCLUSION DU CHAPITRE I

Le droit des données personnelles issu du RGPD se caractérise notamment par la prééminence de la liberté d'entreprendre de l'employeur. Dès lors, le versant protecteur du droit des données personnelles est mis en retrait au profit de la liberté de traitement des données personnelles. La protection des données personnelles des salariés apparaît alors comme un outil d'encadrement de la liberté d'entreprendre, et non comme un objectif à part entière.

Parallèlement, la mise en retrait des mécanismes de protection se justifie par la volonté de renforcer le Marché intérieur. Les données personnelles étant devenues un actif économique favorisant la croissance économique, il est apparu nécessaire d'uniformiser les règles relatives au droit des données personnelles afin de rendre les entreprises européennes compétitives sur le plan international. L'extension du champ d'application de la nouvelle réglementation a alors comme objectif apparent d'aggraver les mécanismes de protection mais aussi celui, caché, d'encourager la compétitivité des entreprises européennes auparavant pénalisées par des règles contraignantes ignorées par les concurrents internationaux.

Confronté à une volonté d'assurer une protection du citoyen-salarié tout en ne souhaitant pas « rater les opportunités économiques du marché numérique³⁶⁷, moteur de croissance en

³⁶³ Il s'agit de la dématérialisation de la procédure Discovery.

³⁶⁴ CNIL, délib. n°2009-474 du 23 juillet 2009. Elle impose que le transfert respecte la Convention de la Haye, mais également le secret professionnel, la légitimité du traitement, le principe de qualité et de proportionnalité des données, la prévisibilité de la durée de conservation des données, le respect des droits et informations des personnes. Le G29 recommande quant à lui et si possible une anonymisation des données.

³⁶⁵ F.NAFTALSKI, *art., préc.*, p.24.

³⁶⁶ R.PERRAY, *art., préc.*, p.61.

³⁶⁷ C.CASTETS-RENARD, *art., préc.*, p.29.

Europe »³⁶⁸, le législateur a dû jouer à l'équilibriste en prenant en compte les contraintes entrepreneuriales. Dès lors les mécanismes de protection s'en sont retrouvé transformés et par extension ceux concernant les salariés.

³⁶⁸ *Ibid*

Chapitre II – La mise en œuvre du droit des données personnelles, source de mutation des mécanismes de protection

Dans la course à la compétitivité et au développement d'une économie numérique³⁶⁹, deux conceptions antinomiques s'affrontaient : celle, française et européenne, qui imposait une réglementation étatique contraignante contre celle, américaine, où les instruments sont sectoriels et où le recours à l'autorégulation était dominant³⁷⁰. Le nouveau droit des données personnelles issu du RGPD a diminué l'écart entre ces deux conceptions puisqu'il a pris acte de l'évolution des procédés de protection.

Cette évolution rend compte de la notion d'Etat-postmoderne³⁷¹. Face à un monde de plus en plus dématérialisé et mondialisé, la puissance d'action des mécanismes de protection traditionnelle n'était pas optimale. Le rôle de l'Etat ne disparaît pas mais se trouve territorialement limité. Pour faire face à cette évolution, il a dû s'adapter et réinvestir son action, non pas dans des mécanismes de puissance publique, mais dans les acteurs eux même³⁷².

C'est pourquoi une mutation des mécanismes de protection est apparue nécessaire tendant à libéraliser (Section 1) et à contractualiser ces derniers (Section 2).

Section 1 – La libéralisation des mécanismes de protection

Les modalités de contrôle du respect de la réglementation sur la protection des données personnelles ont subi de grandes mutations, qui font suite au mouvement de libéralisation des mécanismes de protection opéré depuis quelques années³⁷³.

A la réglementation succède la régulation, et au droit dur succède le droit mou. La libéralisation se traduit alors d'une part, par la mutation de la nature des mécanismes de protection (§1) et d'autre part, par la mutation de leur juridicité (§2).

³⁶⁹ E.BRUNET, *art., préc.*, p.39.

³⁷⁰ L.M AUGAGNEUR, « Vers des nouveaux paradigmes du droit dans l'économie numérique », *RDT com.* 2015, p.455.

³⁷¹ P. MAISANI, F. WIENER, « Réflexions autour de la conception post-moderne du droit », *Droit et société*, n° 27, 1994, p. 443.

³⁷² L. CLUZEL-METAYER ET E. DEBAETS, *art., préc.*, p.1101.

³⁷³ N. OCHOA, *op., cit.*, p. 233.

§1. La mutation de la nature des mécanismes de protection : de la réglementation à la régulation

Si certains considèrent qu'il s'agit d'une révolution, dans les faits il n'en est rien puisque ce passage de la réglementation à la régulation était prédit et suit les différentes évolutions législatives sur ce point. Le RGPD apparaît alors comme l'aboutissement des aspirations. D'une réglementation étatique, le droit se trouve désormais réduit à une régulation à la fois par les entreprises (A), et par les technologies (B).

A. La réduction du droit à une régulation par les entreprises

C'est face au constat de l'impuissance de l'Etat à encadrer des phénomènes relevant de l'initiative d'acteurs privés que le souhait d'une mutation du droit est apparu. Le RGPD a pris acte de cette nécessité en instaurant un régime de régulation, succédant à la réglementation originelle pour plusieurs raisons.

Outre le fait que la réglementation est « assimilée à des entraves au marché économique »³⁷⁴, l'absence de frontière caractérisant le numérique faisait qu'il était compliqué de délimiter une réglementation précise, le cyberspace constituant par nature une zone de non droit, rétive à une réglementation juridique et étatique³⁷⁵.

De même, « la réglementation autoritaire est entravée par de nombreux obstacles : par son uniformité, elle s'adapte mal à la diversité des situations ; par sa stabilité, elle est rapidement frappée d'obsolescence ; par son aspect coercitif, elle suscite des réactions de passivité et de fuite (...). La dérèglementation apparaît alors comme un vecteur de promotions de procédés plus subtils et peut être plus insidieux de contrôle des lois »³⁷⁶. La régulation permettrait d'y remédier car elle serait plus propice à une contextualisation³⁷⁷, et permettrait d'adapter la norme lorsqu'elle s'avère inefficace³⁷⁸. La régulation éviterait alors l'obsolescence programmée de la réglementation.

³⁷⁴ J.L SAURON, *art., préc.*, p.75.

³⁷⁵ G.DESGENS-PASANAU, *art., préc.*, p.25.

³⁷⁶ J.CHEVALLIER, « Régulation et polycentrisme », *La Revue administrative*, 1998, p. 48.

³⁷⁷ G.TIMSIT, « Archipel de la norme », *PUF*, 1997, p. 204.

³⁷⁸ C.CODRON, « La surveillance diffuse : entre Droit et Norme », Thèse 2018, Lille, *CERAPS*, p. 414.

Ainsi, le droit de la régulation serait « un droit pragmatique, sous-tendu par une préoccupation d'efficacité »³⁷⁹. Par régulation, il faut donc « entendre un droit d'en bas, se préoccupant du cas concret »³⁸⁰.

Le RGPD a donc permis le passage de la réglementation à la régulation c'est-à-dire du gouvernement des hommes à la gouvernance par la donnée. Une libéralisation se crée puisque « le propre de la gouvernance est en effet de reposer non pas sur la légitimité d'une loi qui doit être obéie, mais sur la capacité commune à tous les êtres humains d'adapter leur comportement aux modifications de leur environnement pour perdurer dans leur être »³⁸¹.

Si la régulation par les entreprises a atteint son paroxysme avec l'entrée en vigueur du RGPD, il s'avère qu'il ne fait que parachever un mouvement de libéralisation déjà fort présent.

En effet, la libéralisation des mécanismes traditionnels de protection n'est pas soudaine. En ce sens, les formalités préalables ont révélé dès l'origine un système particulièrement libéral et n'ont cessé avec le temps d'accorder une liberté plus grande aux entreprises. L'ancien régime se caractérise par une diminution progressive de la contrainte, que ce soit pour le régime déclaratif³⁸² ou à autorisation préalable³⁸³. Cette croissance d'absence de contrainte est le signe d'un mouvement de libéralisation recherché depuis plusieurs années. Le RGPD ne constitue donc en rien une Révolution.

Parallèlement, face au développement considérable des traitements de données personnelles, il n'était pas réaliste d'imaginer que les mécanismes de formalités préalables soient

³⁷⁹ J. CHEVALLIER, « De quelques usages du concept de régulation », in *MIAILLE Michel (dir.), La régulation entre droit et politique*, L'Harmattan, 1995, p. 85.

³⁸⁰ *Ibid.*

³⁸¹ A. SUPIOT, « La Gouvernance par les nombres », *Cours au Collège de France (2012-2014)*, Fayard, 2015.

³⁸² Le degré de contrainte du régime déclaratif était relativement modeste puisqu'il prenait simplement la forme d'une information du titulaire à la CNIL s'engageant à satisfaire aux exigences de la loi « Informatique et libertés », et précisant la spécificité et les finalités du traitement. Le citoyen-salarié devait également être informé sur l'existence du traitement et de ses droits sur ses données (droits d'accès, de rectification et d'opposition). Ce degré de contrainte s'est encore assoupli avec l'adoption de normes simplifiées par la CNIL consistant en « des modes d'emploi » spécifiques à certains secteurs ou certaines professions » et ne comportant pas d'atteinte à la vie privée ou aux libertés.

³⁸³ La contrainte du régime d'autorisation préalable était également modérée puisque la seule différence avec le régime déclaratif était d'attendre le « feu vert » de la CNIL pour mettre en place le traitement. La contrainte résidait alors dans les délais de traitements des dossiers qui pouvaient prendre plusieurs mois voire plusieurs années. Le degré de contrainte a par la suite été encore allégé puisque « les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une autorisation unique ». Dès lors si c'est le cas, l'entreprise pouvait se contenter d'adresser à la CNIL un engagement de conformité du traitement à la description figurant dans cette autorisation non pas individualisée, mais collective.

systématiquement respectés, étant donné qu'ils ne faisaient pas spécialement l'objet de contrôle de la part de la CNIL³⁸⁴.

La prise en charge de la protection de la vie privée par les entreprises est exactement ce à quoi le RGPD tend. Un renversement de l'effectivité s'opère : la contrainte juridique s'efface au profit de la contrainte exercée par l'entreprise elle-même. Ainsi le RGPD « désinstitue le droit des données personnelles pour y préférer des contre-mesures proposées par les acteurs du marché »³⁸⁵. La protection des citoyens-salariés s'organise dès lors par les entreprises, alors que c'est exactement « à cause » d'elles qu'un régime de protection a été mis en place. Pour combler ce mouvement de libéralisation, les mesures répressives ont toutefois été renforcées³⁸⁶.

La régulation du marché est donc devenue, si ce n'est un objectif, un moyen de protection, ce qui a profondément transformé les modalités d'exercice du pouvoir et du droit. Alors qu'auparavant la réglementation permettait de réguler le marché économique, ce sont désormais les acteurs du marché économique qui régulent la protection.

Cette régulation par les entreprises n'est pas la seule puisque désormais la régulation passe également par les technologies elles-mêmes.

B. La réduction du droit à la régulation par les technologies

La recherche de solutions alternatives à la protection des données personnelles par le droit n'est pas nouvelle. Le recours à la technique ou « lex informatica » apparaît alors comme une solution pour faire face au monde du cyberspace³⁸⁷. Le droit apparaîtrait « comme hypothèse de départ, disqualifié pour non-efficacité »³⁸⁸. Cette recherche s'est concrétisée avec les notions de privacy enhancing technologies (PET's) et la privacy by design and by default. Ces deux notions intègrent la protection de la vie privée dans les technologies elles-mêmes et leurs spécificités. Dès lors, les technologies dans leur construction doivent être à

³⁸⁴ Aux termes de son rapport d'activité publié en 2016 par exemple, 96 323 dossiers de formalités ont été déposés en 2015 dont 50 339 formalités simplifiées.

³⁸⁵ C.CODRON, *op., cit.*, p.336

³⁸⁶ Ces sanctions constituent une mesure d'encadrement par l'Etat des processus de libéralisation. L'intervention de l'Etat n'est pas absente mais s'en trouve simplement modifiée. L'intervention de l'Etat postmoderne passe donc de l'Etat providence à l'Etat régulateur v. J.CHEVALLIER, « Vers un droit postmoderne ? », in *Les transformations de la régulation juridique*, dir.J. CLAM, G.MARTIN, Droit et société n°5, 1998, p. 32. Ainsi en voulant favoriser une logique de régulation, les pouvoirs publics ont néanmoins dotés la CNIL de larges pouvoirs de sanctions. Ce phénomène n'est paradoxal qu'en apparence car l'aggravation d'un pouvoir de sanction s'inscrit dans un « processus général de déréglementation impliquant le passage préventif à des équilibres a priori plus répressifs » v. N. OCHOA, art., préc., p.236.

³⁸⁷ L.CLUZEL-METAYER ET E. DEBAETS, art., préc., p.1101.

³⁸⁸ C.CODRON, *op., cit.*, p.337

même de protéger les données personnelles. Ainsi l'objectif est d'autonomiser les procédés technologiques pour qu'ils puissent par eux-mêmes assurer le respect du RGPD, sans intervention aucune. Bien que controversée³⁸⁹, la régulation par la technique est pertinente puisqu'elle permettrait « une exécution ex ante au lieu d'ex poste »³⁹⁰ et donc, a priori, empêcherait une violation de la réglementation.

Les technologies permettraient d'intégrer en leur sein des algorithmes qui s'ajusteraient sur des nouvelles données collectées et traitées périodiquement en fonction des circonstances. Cette régulation par les technologies permettrait, d'une part, aux entreprises de se soucier du respect de leur pratique à la réglementation RGPD et de s'occuper des traitements les plus sensibles et, d'autre part, à l'Etat de rationaliser son rôle à des missions spécifiques comme le traitement de données personnelles tenant à la sécurité de l'Etat. Ainsi le rôle de l'Etat dans la protection des données se limiterait aux missions régaliennes qui lui incombent. L'Etat s'en retrouverait alors plus performant.

Si cette déréglementation successive impacte la protection des données personnelles des citoyens-salariés sur les technologies elles-mêmes, il ne faut pas voir l'innovation technologique comme une fatalité étant donné que de nombreux services existent sans collecter abusivement les données personnelles. Il faut alors repenser l'innovation au prisme de la protection par la technique³⁹¹.

Outre les moteurs de recherche comme Qwant ou les réseaux sociaux comme Whaller, la « blockchain »³⁹² est l'illustration parfaite et l'exemple le plus abouti de la désintermédiation au profit de la technologie. Cette dernière permettrait de garantir l'anonymat en certifiant de manière absolue l'intégralité des échanges, sans recours à un tiers de confiance. Les risques de piratage sont donc extrêmement faibles. Cependant, il s'avère qu'une étude de la CNIL met en

³⁸⁹ V. Partie 1, Chapitre I, section 2, §1, B) une garantie contre l'objectivation du salarié.

³⁹⁰ C.CODRON, *op. cit.*, p.337

³⁹¹ I. REGNAUD, auteure du blog « Mais où va le web », dans son billet « Revendre ses données personnelles, la fausse bonne idée », 2018.

³⁹² Vocabulaire de l'informatique, JO 23 mai 2017, texte n°20 : la blockchain est « un mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification ». V. définition F.CHAFIOL ET A.BARBET-MASSIN, « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *Dalloz IP/IT*, 2017 : « La blockchain est une technologie de stockage et de transmission distribuée de transactions, qui fonctionne de pair-à-pair, sans tiers de confiance et sans administrateur central de contrôle. Cette dernière se matérialise par une chaîne de blocs, regroupés en transactions, qui sont vérifiés (techniques de cryptographie asymétrique en fonction de hachage) puis validés (algorithme de consensus distribué) par les nœuds du réseau, c'est-à-dire par les participants. Ces transactions sont ensuite accessibles sur un livre virtuel, ouvert et infalsifiable ».

avant l'incompatibilité entre cette technologie et certaines dispositions du RGPD³⁹³. Tout d'abord, la CNIL met en garde contre l'absence de responsable de traitement, par définition absente de la blockchain, qui réduirait les possibilités de contrôler matériellement ce que font les parties prenantes³⁹⁴. Le responsable de traitement, selon la CNIL, serait alors la personne qui « décide » d'inscrire une donnée personnelle dans la blockchain, ce qui reviendrait à faire peser l'intégralité de la protection sur la personne elle-même. Ensuite, le droit à l'oubli serait pour ainsi dire oublié. La blockchain est construite autour du « principe d'immutabilité des données gravées au sein de ses blocs »³⁹⁵, par définition essentiel à la lutte contre le piratage et la fraude. Néanmoins, si certains principes peuvent apparaître incompatibles avec le RGPD, d'autres en revanche, peuvent parfaitement être respectés par la blockchain. En effet, le droit d'accès, par exemple, est garanti par le caractère par définition transparent de ces technologies. De même, la blockchain est peu identifiante car il s'agit de numéros uniques ne permettant pas à eux seuls d'associer un nom ou un visage. Ainsi, si certaines dispositions plaident en faveur d'une incompatibilité entre la blockchain et le RGPD, il n'en demeure pas moins que la blockchain suit les mêmes finalités que les règles actuelles, à savoir la protection des personnes contre les abus des entreprises dans un univers centralisé. Or justement, la blockchain est la « promesse d'un espace d'échanges décentralisé où le tiers de confiance n'est plus nécessaire »³⁹⁶.

Ainsi, le « gouvernement le meilleur » ne serait-il pas « celui qui gouverne le moins »³⁹⁷ ? Il ne faut cependant pas conclure au retrait total de l'Etat. Le recours à la technique ne doit pas être exclusif d'autres mécanismes de protection. Il serait alors aberrant de croire en un « solutionnisme technologique »³⁹⁸.

En définitive, cette suppression des formalités préalables a entraîné le passage d'une réglementation étatique à une régulation par les acteurs du marché et les technologies. Cette suppression s'est également accompagnée de l'augmentation de procédés de substitution d'inspirations postmodernes, bien qu'ils fussent déjà fort présents avant l'abolition officielle des formalités préalables. En effet, pour préserver une protection des données

³⁹³<https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles>

³⁹⁴ T. DOUVILLE, « Blockchain et protection des données à caractère personnel », *AJ contrat* 2019, p. 316 : il existerait une « incompatibilité intellectuelle d'abord, l'architecture de la blockchain est décentralisée – elle repose sur un réseau de pair à pair – tandis que le droit des données personnelles est construit autour d'un acteur central qui est le responsable de traitement ».

³⁹⁵ T. DOUVILLE, *art., préc.*, p.316.

³⁹⁶ S. NAILLAT, « La blockchain, un risque pour les données personnelles ? », *in* La Tribune, 2018.

³⁹⁷ H-D THOREAU, « La désobéissance civile », *Culture Commune*, 2014, p. 1.

³⁹⁸ C.CODRON, *op.,cit.*, p. 406.

potentiellement affaiblie par la politique de libéralisation du droit des données personnelles, des mesures compensatoires ont été adoptées rendant compte de la tendance postmoderne du droit des données personnelles. Cette tendance de transformer les mécanismes originels de protection par des procédés de privatisation des opérations de contrôle ou par des procédés empruntant au droit mou, n'est pas nouvelle et ne constitue en réalité qu'une « ruse de l'Etat postmoderne », lui permettant d'affermir son contrôle³⁹⁹. La juridicité des mécanismes de protection s'en trouve alors modifiée.

§2. La mutation de la juridicité des mécanismes de protection : du droit dur au droit mou

Si les missions de l'Etat se sont développées et diversifiées dans le cadre de l'Etat providence, le progrès numérique et technologique a conduit à rechercher l'efficacité du système de protection à travers d'autres mécanismes a-juridiques. Ce recul de l'Etat se fait sentir, à la fois par le recours à la privatisation (A) mais également par le recours à des procédés extra-juridiques (B).

A. La privatisation des mécanismes de contrôle

Cette privatisation passe à la fois par une participation accrue du contrôlé à son propre contrôle, et par l'institution d'un DPD (1). Cependant cette privatisation ne pourrait pas s'exercer, ou en tout cas ne recevrait pas des louages, si des actions de sensibilisation et de formation n'étaient pas organisées (2).

1) La privatisation par les procédures de contrôle interne

Tout d'abord, la participation du citoyen-salarié à son propre contrôle est apparue avantageuse pour l'Etat en raison des faibles coûts qu'elle induit. Cette participation s'analyse en un partage « de la charge de la régulation » entre l'Etat et les entreprises⁴⁰⁰. Si ce partage est apparu avantageux pour l'Etat, il en est autrement pour le citoyen-salarié étant donné que dans le cadre de la relation de travail, le salarié ne dispose pas d'une force de persuasion. Ce report du contrôle se traduit également par une obligation de notifier à la CNIL une violation des données personnelles constatée⁴⁰¹, et ce avec l'aide des représentants des salariés qui

³⁹⁹ N.OCHOA, *op., cit.*, p. 234

⁴⁰⁰ N.OCHOA, *op., cit.*, p.249.

⁴⁰¹ Règl.n°(UE) 2016/679, *op., cit.*, art. 33.

disposent du droit d'alerte. La force de persuasion prend alors ici de l'ampleur même si ce droit d'alerte est à relativiser⁴⁰².

Ensuite, l'institution d'un Correspondant Informatique et Libertés (CIL) a également marqué le passage progressif vers une certaine privatisation puisque ce dernier « exerçait par une délégation implicite certains pouvoirs qui incombent » à l'Etat⁴⁰³. A ce CIL, facultatif, a succédé le DPD, parfois obligatoire. Cette tendance traduit « une extension des procédures de contrôle interne au détriment des procédures de contrôle externe »⁴⁰⁴. Le DPD est alors conçu, dans un rôle rappelant celui du représentant du personnel, comme l'interlocuteur privilégié au sein de l'entreprise en devant « être associé d'une manière appropriée et en temps utiles à toutes les questions relatives à la protection des données personnelles »⁴⁰⁵. Il constitue alors une « fonction-support et un substitut fonctionnel »⁴⁰⁶ de la CNIL en interne. Pour le Conseil d'Etat, ce procédé présente un intérêt particulier puisqu'il « assure le respect de la loi de manière continue et pas seulement au stade de l'obligation formelle de déclaration »⁴⁰⁷.

Derrière une volonté de protection s'est en réalité caché un objectif de réduction des coûts sur les opérations de contrôle. Cependant privatiser sans s'assurer d'un niveau de sensibilisation et de formation adéquate aurait alors augmenté les risques d'atteintes à la protection des données personnelles des salariés.

2) La privatisation par les actions de sensibilisation et de formation

Cette privatisation, pour qu'elle soit efficace, nécessite en amont l'identification des salariés au sein de l'entreprise qui traitent des données personnelles ou qui ont vocation à en collecter. Presque tous les salariés de l'entreprise en somme. Une fois un groupe de salariés identifié, il faudra alors le sensibiliser aux nouveaux enjeux du RGPD et former véritablement

⁴⁰² C.trav., art.L.4131-2 : « Le représentant du personnel au comité social et économique, qui constate qu'il existe une cause de danger grave et imminent, notamment par l'intermédiaire d'un travailleur, en alerte immédiatement l'employeur selon la procédure prévue au premier alinéa de l'article L. 4132-2 ». Ce droit d'alerte est à relativiser puisque, d'une part, il repose sur l'espoir d'un sursaut de l'employeur alerté sur les menaces à venir et d'autre part, il s'agit d'un droit et non d'un devoir ou d'une obligation d'alerte. La responsabilité du CSE ne peut donc pas être engagée.

⁴⁰³ N.OCHOA, *op., cit.*, p.249.

⁴⁰⁴ N.OCHOA, *op.,cit.*, p. 250.

⁴⁰⁵ *Ibid.*

⁴⁰⁶ *Ibid.*

⁴⁰⁷ CE, « Le numérique et les droits fondamentaux », *La Documentation Française*, 2014, p. 177-178

le personnel ayant un accès permanent ou régulier aux données personnelles⁴⁰⁸. Cette charge repose sur l'employeur lui-même ou par délégation sur le DPD.

Ces actions de sensibilisation et de formation sont indispensables d'une part, car elles permettent à l'entreprise de démontrer qu'elle a pris les mesures nécessaires pour que son personnel veille au respect de la réglementation RGPD lorsqu'ils manipulent des données⁴⁰⁹, et d'autre part, car la complexité et technicité de la réglementation nécessite « une bonne maîtrise des connaissances et une mise à jour régulière, une capacité de décryptage et, de veilles juridique et technologique »⁴¹⁰.

Pour être pragmatique, l'employeur devra adapter le niveau de sensibilisation et de formation au regard des connaissances et compétences techniques du personnel. Un travail d'individualisation est donc indispensable à une sensibilisation et une formation efficace. Dès lors, ces actions peuvent prendre diverses formes allant du simple kit d'accueil⁴¹¹ à la réalisation de formations diplômantes⁴¹² ou non⁴¹³, en passant par la mise à disposition d'informations et d'explications sous format papier, ou disponibles sur l'intranet de l'entreprise dédié spécifiquement à cet effet.

Outre les organismes privés⁴¹⁴, le milieu universitaire s'est également emparé de cette question en développant les offres de formation⁴¹⁵. Pour l'instant, le conservatoire des arts et métiers est le seul organisme de formation en France qui bénéficie du label « CNIL formation »⁴¹⁶, qui a d'ailleurs été actualisé récemment en raison de l'adoption du RGPD⁴¹⁷. Les associations professionnelles sont également dans la course et quoi de mieux que des professionnels qualifiés pour mettre en place leurs propres dispositifs⁴¹⁸.

⁴⁰⁸ Règl.n°(UE) 2016/679, *op.,cit.* art 42.

⁴⁰⁹ G.DESGENS-PASANAU, « Formation et sensibilisation des nouveaux acteurs : quelles solutions ? », JA 2018, n°571, p.27. C'est important en cas de contrôle de la CNIL ou de procédure contentieuse car la bonne foi de l'employeur est prise en compte.

⁴¹⁰ *Ibid.*

⁴¹¹ Ce kit d'accueil, pourra être remis à chaque nouveau salarié entrant dans l'entreprise et devra préciser les enjeux du RGPD, les procédures internes applicables et le rôle du DPD.

⁴¹² La formation diplômante ou certifiante est un plus pour le DPD qui doit justifier d'un niveau de compétence en droit des données personnelles

⁴¹³ Ici il est fait référence aux sessions de formations en présentiel ou en e-learning qui peuvent être générales ou alors évoquer des points précis.

⁴¹⁴ Le mastère en formation et protection des données personnelles délivrées par ISEP.

⁴¹⁵ En témoigne la création récente du diplôme universitaire de la Sorbonne, « Data Protection Officer ».

⁴¹⁶ Récemment actualisé pour tenir compte de l'entrée en vigueur du RGPD. V. CNIL, délib. n°2017-220 du 13 juillet 2017 venant remplacer CNIL, délib. n°2011-315 du 6 octobre 2011.

⁴¹⁷ CNIL, délib. n°2017-220 du 13 juillet 2017 venant remplacer son CNIL, délib. n°2011-315 du 6 octobre 2011.

⁴¹⁸ Le dispositif de l'International Association of Privacy Professionals, IAPP Europe regroupe les DPO issus d'entreprises américaines présentes en Europe. L'IREO de Lille devra alors certainement prévoir d'adapter ses formations pour être dans l'air du temps RGPD.

En définitive, il résulte que l'évolution post-moderne du régime applicable en matière de protection des données personnelles impliquant une privatisation des opérations de contrôle est plutôt avancée. Si cette évolution constitue la trame de cette « post-modernité », cette dernière ne sera complète que si des procédés extra-juridiques sont introduits au sein de ce régime de protection.

B. Les procédés extra-juridiques des mécanismes de protection

Il ne faut pas oublier que l'objet du droit des données personnelles est d'assurer la liberté d'entreprendre de l'employeur, tout en essayant de blinder la protection des données personnelles et ce, dans un objectif de renforcement du Marché intérieur. Dès lors, la postmodernité du droit des données personnelles se traduit également par le développement de procédés a-juridiques.

L'objectif est de diluer la force obligatoire du droit, voire à l'estomper totalement pour que certains mécanismes de protection puissent s'appliquer sans être touchés par la règle de droit. Le recours au droit mou (« soft law ») en constitue un outil « dans une perspective de contrôle non contraignant de la légalité »⁴¹⁹.

Les missions de la CNIL d'information du public et des représentants nationaux trouvent ici toute leur importance. D'une part, en présentant son rapport annuel chaque année, la CNIL offre aux citoyens une information théorique et pratique sur les risques que présentent les nouvelles technologies⁴²⁰. D'autre part, en rendant public des avis sur « l'évolution des technologies de l'information », la CNIL se veut la « conscience sociale » de la société en lieu et place des représentants nationaux⁴²¹.

Si ces deux procédés sont dénués de portée juridique, ils jouissent d'une grande publicité. La fabulation est toutefois à éviter puisque rendre public ces informations ne peut être dans l'absolu considéré comme totalement efficace, si ce n'est multiplier l'effet préventif en informant les autres entreprises des critères juridiques exigés.

En passant à une logique de conformité, le RGPD encourage le développement d'outils d'accompagnement des entreprises. Cette approche dite « fondée sur le risque » pourra être facilitée par l'adhésion à des codes de conduites⁴²², certifications⁴²³ qui succèdent aux

⁴¹⁹ C.TESTARD, « Le droit souple, une « petite » source canalisée », *AJDA* 2019, p. 934.

⁴²⁰ L. CLUZEL-METAYER ET E. DEBAETS, *art., préc.*, p.1101.

⁴²¹ N.OCHOA, *op., cit.*, 264.

⁴²² Règl.n°(UE) 2016/679, *op., cit.*, art 40.

⁴²³ Règl.n°(UE) 2016/679, *op., cit.*, art 42.

labellisations, et le suivi scrupuleux des recommandations et guides de bonnes pratiques établis par la CNIL. La RGPD a donc sensiblement modifié la donne. Promouvant l'application de ces procédés, la volonté est d'asseoir des alternatives au droit dur qui n'avait jusque là pas spécialement portée ses fruits en matière de protection des données jusqu'ici⁴²⁴.

Les codes de conduite rédigés par les acteurs professionnels (associations ou organisations professionnelles), permettent de préciser les modalités d'application du RGPD sur certains points, dont notamment la durée de conservation, les modes opératoires, les notions de traitement loyal, transparent, etc. Soumis à l'avis de la CNIL, ces derniers sont publiés par elle et permettent aux acteurs du marché d'y adhérer. En cas de violation du code de conduite, l'organisme chargé du contrôle pourra lever l'application du code et « devra informer la CNIL de ces mesures et des raisons pour lesquelles elles ont été prises ».

A la labellisation⁴²⁵ a succédé la certification. Si cette dernière peut être accordée par un organisme de certification agréé⁴²⁶, elle peut également l'être par la CNIL ce qui est surprenant car elle cumulerait ici les fonctions de « certificateur et de contrôleur »⁴²⁷. La question de la conciliation entre ces deux nouvelles missions se « posera sans doute lorsqu'il s'agira de sanctionner une organisation qu'elle aura certifiée en amont »⁴²⁸.

Cependant il convient de préciser que ces mécanismes n'offrent qu'une protection restreinte pour l'employeur puisque la certification tout comme l'adhésion à un code de conduite ne diminue pas sa responsabilité⁴²⁹ mais permet d'être pris en compte dans le prononcé d'une sanction⁴³⁰.

De même, la CNIL peut publier des « guides de bonne pratique »⁴³¹, recommandations dans plusieurs domaines permettant d'accompagner les employeurs et employés dans leurs pratiques quotidiennes. Parmi ces guides, cinq concernent la relation de travail⁴³². Un travail de vulgarisation doit donc être opéré pour que chaque acteur puisse en comprendre les termes.

⁴²⁴ N.METALLINOS, A. DEBET, J.MASSOT ET N.METALLINOS, « Informatique et libertés. La protection des données à caractère personnel en droit français et européen », *Lextenso*, coll. « Les intégrales », 2015, spéc.n°379 et s.

⁴²⁵ Loi n° 78-17 du 6 janvier 1978, art 11, 3 c.

⁴²⁶ Les organismes sont agréés quand ils démontrent « à la satisfaction de l'autorité de contrôle compétente, leur indépendance et leur expertise au regard de l'objet de la certification ». L'article 43 prévoit plusieurs critères dont évidemment l'inexistence du moindre conflit d'intérêts. Cet agrément est délivré pour une durée de 5 ans maximum.

⁴²⁷ L.CLUZEL-METAYER ET E. DEBAETS, *art., préc.*, p.1101.

⁴²⁸ O.TAMBOU, « L'introduction de la certification dans le RGPD : quelle valeur ajoutée ? », *RLDI*, 2016, n°3969, p.43.

⁴²⁹ Règl.n°(UE) 2016/679, *op., cit.*, art 42.4.

⁴³⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 82.2.

⁴³¹ Règl.n°(UE) 2016/679, *op., cit.*, art 35.

⁴³² V. les guides pratiques se référant au recrutement, au contrôle des horaires et de l'accès aux bureaux, à l'utilisation d'Internet et de la messagerie, et aux dispositifs de géolocalisation et de vidéo-surveillance

Si l'objectif de la CNIL est de limiter le risque contentieux, sa volonté et son ambition s'arrêtent à celles des employeurs et employés qui doivent également fournir des efforts pour rendre effectifs ces guides de bonnes pratiques dans l'entreprise.

Du point de vue de l'entreprise, l'évolution des mécanismes de droit mou est considérable puisque ses actions étaient jusqu'à présent « plutôt orientées vers la stigmatisation des entreprises en infraction avec la réglementation »⁴³³.

Le respect de la protection des données personnelles des citoyens-salariés deviendrait-elle comme l'a pertinemment fait remarquer Clémence Codront, une marque, un label au « même titre que le label bio est apposé sur les œufs de poules élevées en plein air ? »⁴³⁴, exigeant le strict minimum alors que nous savons pertinemment l'horreur que sous-tend le commerce des poules pondeuses ?

Si la compétence de la CNIL était auparavant principalement centrée sur l'instruction des dossiers de déclarations et d'autorisations, elle devra désormais s'engager dans une démarche d'éducation numérique et de communication, afin d'élaborer un certain nombre de recommandations précises et techniques permettant d'assurer la sécurité juridique de l'employeur. Or, si la fin des formalités préalables constitue un enjeu majeur de changement de conduite pour la CNIL, le nombre d'agents n'a pas augmenté. A titre de comparaison, l'autorité de contrôle britannique, l'Information Commissioner's Office, compte environ 700 agents contre 200 en France⁴³⁵. Il s'avère donc indispensable pour les pouvoirs publics de renforcer les moyens de la CNIL afin qu'elle puisse disposer des ressources humaines nécessaires à l'exercice de sa mission.

En définitive, il est possible d'affirmer d'une part, que ces « nouveau » dispositifs « constituent une grille juridique pour apprécier la régularité d'un dispositif de traitement » et d'autre part, qu'ils forment « un volet juridique adaptable à notre environnement numérique »⁴³⁶.

Par ailleurs, en calquant sa réglementation sur la culture type anglo-saxonne pour lequel le droit est fondé sur une relation de confiance : le contrat plutôt que la loi, les mécanismes empruntant aux procédés de l'Etat post-moderne questionnent le rôle de l'Etat dans la production normative. Si le RGPD est l'aboutissement de la libéralisation des mécanismes de

⁴³³ G. DESGENS-PASANAU, *art., préc.*, p.262.

⁴³⁴ C.CODRON, *op., cit.*, p.311.

⁴³⁵ G.DESGENS-PASANAU, « La protection des données personnelles, le RGPD et la loi française du 20 juin 2018 », LexisNexis, 2019, p.173.

⁴³⁶ G.LOISEAU, « Your employer is watching you », *Cah.soc.*, 2013, n°255, p.333.

protection, il s'avère qu'il accompagne également une évolution tendant à une contractualisation des mécanismes de protection.

Section 2 – La contractualisation des mécanismes de protection

La protection des données personnelles entretient des liens plutôt étroits avec la notion de contractualisation. En effet, dans le cadre des relations de travail, le recours au droit négocié se voit accorder une place importante (§1). Cette contractualisation atteint son apogée lorsque l'idée d'une vie privée négociée se propage (§2).

§1. Le droit négocié

Puisque « la vie privée a cessé d'être un droit individuel pour devenir une négociation collective »⁴³⁷, il est nécessaire de dé-judiciariser la défense de cet intérêt collectif tout en s'assurant qu'une dose de moyens d'actions collectifs soit réinjectée (B).

A. La déjudiciarisation de la défense d'intérêt collectif

La déjudiciarisation passe à la fois par le recours à la négociation collective (1) mais également par le recours aux chartes d'entreprises (2).

1) Le recours à la négociation collective

Actuellement les espaces de négociation propices à la gouvernance des données collectées font défaut. Dans le cadre de la relation de travail, le RGPD en fait pourtant la promotion et offre la possibilité de porter la protection des données au sein des conventions collectives. L'article 88 du RGPD prévoit en effet que les conventions collectives peuvent venir préciser des garanties apportées au respect des droits des travailleurs en ce qui concerne le traitement de leurs données personnelles⁴³⁸.

⁴³⁷ A. CASILLI ET P.TUBARO, Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée *in* Conseil d'État, Le numérique et les droits fondamentaux, 2014.

⁴³⁸ Règl.n°(UE) 2016/679, *op.cit.*, art 88 : « Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens

Si cette possibilité n'était pas exclue, la directive de 1995 et la loi « Informatique et Libertés » n'y faisaient pas expressément référence contrairement à l'Allemagne par exemple, où le recours aux négociations collectives est privilégié notamment par le fait que les partenaires sociaux disposent de véritables prérogatives et d'un pouvoir d'influence sur les décisions de l'employeur⁴³⁹.

Le considérant 155 du RGPD vient préciser qu'en plus des conventions collectives, des accords d'entreprises pourront également tenir lieu de règles spécifiques mises en place au sein de l'Etat membre pour protéger les salariés dans le cadre de leurs relations de travail⁴⁴⁰.

La protection des données personnelles des salariés devient alors un enjeu de négociation syndicale et de démocratie sociale. La protection des données pourra faire l'objet « d'une déclinaison sectorielle »⁴⁴¹ en fonction des dispositifs de traitement des données personnelles mis en place au sein de l'entreprise. L'opportunité de mettre en place un dispositif de traitement, le choix de ce dispositif, les méthodes de collecte et les catégories de salariés et données concernés relèveront non plus d'une décision unilatérale de l'employeur (bien que les représentants du personnel aient été t consultés sur ce sujet) mais d'une décision négociée avec les partenaires sociaux.

Des garanties supplémentaires viendront alors s'ajouter au socle légal, ce qui permettra de compenser le déséquilibre induit par la relation de travail. L'intérêt légitime de l'entreprise ne sera alors vraiment « légitime » que s'il est collectivement débattu selon les principes de la démocratie sociale et à condition que les syndicats s'emparent de cet enjeu.

appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail. Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail ».

⁴³⁹ Le comité d'entreprise allemand (Betriebsrat), obligatoire dès lors que le seuil d'effectif de l'établissement dépasse cinq salariés, dispose d'un droit de véto (Widerspruchsrecht) notamment concernant les mesures individuelles des salariés. L'employeur est tenu de respecter la décision du comité. Le caractère contraignant de la consultation du comité rend alors la négociation collective efficace.

⁴⁴⁰ Règl.n°(UE) 2016/679, *op.cit.*, considérant 155 : « Le droit des États membres ou des conventions collectives, y compris des «accords d'entreprise» peuvent prévoir des règles spécifiques relatives au traitement des données à caractère personnel des employés dans le cadre des relations de travail, notamment les conditions dans lesquelles les données à caractère personnel dans le cadre des relations de travail peuvent être traitées sur la base du consentement de l'employé, aux fins du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, et aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail ».

⁴⁴¹ C.SCHULTIS, « Le traitement de données dans le cadre des relations de travail dans le règlement sur la protection des données personnelles », *Daloz IP/IT*, 2017, p. 265

Cette protection doit donc devenir un enjeu syndical et de négociation collective puisqu'il n'est pas sans importance de rappeler qu'entre 5% et 20% des plaintes adressées à la CNIL chaque année concernent les relations entre les salariés et leurs employeurs, notamment à propos du contrôle de l'usage de leurs données personnelles et du droit d'accès auxdites données⁴⁴².

Les conventions ou accords collectifs ne sont pas les seules à permettre le retour à un droit négocié et contractualisé. Trouvent ici leur place les chartes d'entreprises.

2) Le recours aux chartes d'entreprises

L'utilisation de l'outil informatique peut occasionner des difficultés pratiques. Dès lors, ces chartes permettent, non seulement d'assurer une parfaite information des salariés sur leurs droits lors de l'utilisation de l'outil professionnel (notamment à des fins personnelles), mais également sur le comportement qu'ils doivent adopter quand ils utilisent l'outil informatique (durée de connexion à titre privée, sites prohibés, etc.)⁴⁴³. Toutefois, elles ne doivent pas être instrumentalisées pour prohiber l'utilisation personnelle des outils professionnels, ou alors organiser une liste fastidieuse de restrictions. Le risque est en effet de produire l'effet inverse de celui recherché, à savoir la dilution d'une information concise dans une masse d'informations éparses.

Les représentants de la démocratie sociale en entreprise trouvent ici un rôle important puisqu'ils devront être associés à la rédaction pour que cette dernière puisse être opposable au salarié⁴⁴⁴. En revanche la charte n'a, en principe, pas de valeur contraignante. Pour lui en donner une, il est donc préférable de l'annexer au contrat de travail ou au règlement intérieur de l'entreprise. L'annexion de la charte au contrat de travail impose la signature d'un avenant au contrat pour chaque salarié de l'entreprise, ce qui en pratique peut s'avérer compliqué. La deuxième proposition est donc préférée car, même si les formalités de mise en place sont plus importantes (recueil de l'avis des représentants du personnel, transmission à l'inspecteur du travail, information des salariés), l'annexion de la charte au règlement informatique aura

⁴⁴² Aux termes de ses rapports d'activités publiés chaque année.

⁴⁴³ Par exemple, la Charte éthique et numérique RH, proposée par le syndicat CFE-CGC et le Lab RH a pour objectif d'accompagner l'entrée en vigueur du RGPD en formulant des principes à respecter lors de la mise en œuvre des dispositifs de traitement de données notamment les traitements algorithmiques. Son renvoi à l'article 88 du RGPD permet d'inciter les partenaires sociaux à conclure des conventions collectives.

⁴⁴⁴ V.DUEZ-RUFF, « Impact des nouvelles technologies sur le droit du travail : un salarié appartient-il virtuellement à son employeur ? », *Lexbase Hebdo* éd. Soc. n°498, 2012.

l'avantage d'être opposable à tous les salariés⁴⁴⁵. Dès lors, si le document ne respecte pas les conditions d'élaboration du règlement intérieur, il ne pourra pas être opposable au salarié⁴⁴⁶. Son annexion au règlement intérieur présente un intérêt pratique. Défini à l'article L.1321-1 du Code du travail⁴⁴⁷, le règlement intérieur peut venir encadrer l'usage à titre personnel des outils mis à la disposition des salariés en prévoyant une échelle de sanctions. Si le règlement intérieur impose la présence du salarié lors de l'ouverture d'un fichier, l'employeur ne pourra s'y soustraire, sauf motif impérieux dûment justifié. C'est pourquoi, la chambre sociale de la Cour de cassation rappelle à plusieurs reprises qu'est illicite le moyen de preuve qu'un employeur s'est constitué en consultant les messages électroniques des salariés au motif que « le règlement intérieur de l'entreprise prévoyait que les messageries électroniques des salariés ne pouvaient être consultées par la direction qu'en présence du salarié »⁴⁴⁸. Ainsi, si les courriels adressés ou reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel en permettant à l'employeur de les ouvrir hors de la présence de l'intéressé, sauf s'ils sont identifiés comme personnels, le règlement intérieur peut venir restreindre le pouvoir de consultation de l'employeur en le soumettant à d'autres conditions.

Ainsi, en cas de licenciement fondé sur une méconnaissance par le salarié ou l'employeur des dispositions d'une charte, il ne faut pas manquer de s'interroger sur la valeur de cette charte et son opposabilité au salarié, à défaut le licenciement sera sans cause réelle et sérieuse.

Si la voie du dialogue social est une voie à privilégier pour parvenir à une protection des données personnelles au travail, il est nécessaire que les négociants disposent de moyens d'actions pour y parvenir.

B. La réinjection de moyens d'actions collectifs

⁴⁴⁵ C.trav., art.L.1321-5 : « Les notes de service ou tout autre document comportant des obligations générales et permanentes dans les matières mentionnées aux articles L.1321-1 et L.1321-2 sont, lorsqu'il existe un règlement intérieur, considérées comme des adjonctions à celui-ci. Ils sont, en toute hypothèse, soumis aux dispositions du présent titre ». Dès lors peu importe l'intitulé donné aux documents dès lors que le contenu de la charte relève du champ du règlement intérieur, c'est-à-dire comportant des règles relevant de la discipline et entraînant des risques de sanctions, ces chartes peuvent venir servir de support à une éventuelle sanction disciplinaire.

⁴⁴⁶ Conseil de Prud'hommes de Paris, 10 juin 2014, n°13/02093.

⁴⁴⁷ C.trav., art. L. 1321-1 du Code du travail : « le règlement intérieur est un document écrit émanant du chef de l'entreprise, qui contient exclusivement les mesures d'application de la réglementation en matière d'hygiène et de sécurité, les règles générales et permanentes relatives à la discipline et notamment la nature et l'échelle des sanctions, les dispositions relatives aux droits de la défense des salariés susceptibles d'être sanctionnés... ».

⁴⁴⁸ Cass. soc., 26 juin 2012, n°11-15.310.

Le recours à des moyens d'actions collectifs peut s'exprimer de deux sortes : d'une part en ayant recours à des actions de groupe (1) et d'autre part, en ayant recours aux actions syndicales pour inciter à la conclusion de conventions collectives (2).

1) Le recours aux actions de groupe

Tout d'abord, les actions de groupe (ou « class actions ») permettent aux salariés de déléguer la défense de leurs droits et libertés fondamentaux à leurs représentants afin de faire valoir leurs droits devant la justice. Ce mécanisme, déjà introduit en France en matière de protection des données personnelles par la loi de modernisation de la justice du XXI^e siècle⁴⁴⁹ a été renforcé par le RGPD⁴⁵⁰ et la nouvelle loi « Informatique et Libertés »⁴⁵¹.

En effet, initialement limitée à la constatation et à la cessation d'un manquement du responsable de traitement ou de son sous-traitant, l'action collective est désormais étendue à la réparation des préjudices individuels matériels et moraux⁴⁵².

Cet élargissement de l'action de groupe compense alors l'approche individualiste de l'empowerment inhérente au RGPD⁴⁵³ et se justifie par la volonté de rendre « effectives ces actions en matière de protection des données »⁴⁵⁴ même, s'il est fort à « parier qu'une simple addition de revendications de droits individuels puisse déboucher à elle seule sur une action réellement collective⁴⁵⁵ ». En effet, s'il y a bien un « groupe procédural », il agit en revanche « en coalition de cas particuliers puisque chacun continue à porter son propre intérêt individuel ».

Dès lors, si cette action de groupe permet d'obtenir la réparation de préjudices individuels, il n'est pas à rejeter l'idée d'aboutir à une réparation du préjudice moral collectif permettant d'aborder la dimension collective de la protection des données personnelles « transcendant alors l'intérêt collectif de la société »⁴⁵⁶.

L'action de groupe n'est pas le seul moyen d'action collectif puisqu'il existe les traditionnelles actions syndicales.

⁴⁴⁹ Loi n° 2016-1547 du 18 nov. 2016 de modernisation de la justice du XXI^e siècle, JORF n°0269 du 19 novembre 2016.

⁴⁵⁰ Règl.n°(UE) 2016/679, *op., cit.*, art 80.1

⁴⁵¹ C'est par un amendement que l'action collective a été en partie renforcée comme le souhaitait la CNIL V. CNIL, délib n° 2017-299 du 30 novembre 2017.

⁴⁵² Loi n°2018-493, 20 juin 2018, *op.,cit.*, art 43 ter et 43 quater.

⁴⁵³ V. PEUGEOT, dans son billet : « RGPD : quelle place pour l'action collective ? » 2018.

⁴⁵⁴ L.CLUZEL-METAYER ET E.DEBAETS, *art., préc.*, p.1101.

⁴⁵⁵ J.ROCHFELD, dans son billet : « l'action de groupe est-elle vraiment collective ? » 2018.

⁴⁵⁶ C.ZOLYNSKI, « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », *Dalloz IP/IT* 2018, p.470.

2) Le recours aux actions syndicales

Tout d'abord, les employés disposent du droit de grève. Ils disposent donc de moyens de pressions pour déclencher des « conflits sociaux » et « obliger » les entreprises récalcitrantes à conclure des accords sur la protection des données personnelles.

Cependant, le droit de grève est souvent critiqué pour son manque d'efficacité. La CNIL pourrait ici retrouver un rôle décisif. En effet, puisqu'elle dispose de pouvoirs de mise en demeure et de sanctions activables qui ont été considérablement renforcés avec le RGPD, il n'est pas sans intérêt d'imaginer que ce pouvoir de mise en demeure puisse être utilisé pour obliger les entreprises en infraction à entrer dans un processus de négociation avec les partenaires sociaux. Le droit de grève, qui a subi des coups durs ces dernières années, retrouverait alors en efficacité et les syndicats en crédibilité.

Ensuite, il faudrait redonner aux partenaires sociaux des moyens financiers pour qu'ils puissent jouer leur rôle efficacement. D'une part, la conclusion de conventions ou accords collectifs sur la protection des données personnelles exige des connaissances et compétences spécifiques. Ces conclusions obligeraient alors à substituer l'épithète « social » limité aux problématiques faisant l'objet de négociations obligatoires à celui de « sociétal » qui engloberait la dimension collective de la protection des données personnelles.

Si ce dialogue permettrait de substituer l'engagement unilatéral de l'employeur à un engagement sur une base contractuelle négociée, le risque est de voir des sujets traités de façon superficielle dans le cadre d'une négociation collective éclatée.

Il faudrait donc assurer une formation théorique et pratique aux syndicats pour qu'ils puissent débattre efficacement et en connaissance de cause.

De même, il faudrait que succède à l'avis consultatif un avis délibératif, voire instaurer un véritable droit de véto, à l'image de nos voisins nordiques, pour rendre performante et crédible la négociation collective.

En définitive, la divergence des régimes et des mécanismes de protection des données personnelles des salariés, ainsi que le « millefeuille » de réglementations applicables pouvant aller jusqu'à la conclusion de conventions et accords, peuvent participer à la confusion. Certains ont donc émis l'idée d'« ubériser » la vie privée afin que les données personnelles des citoyens-salariés puissent être protégées face au traitement massif et sans limites opérés par les entreprises. Le recours à une vie privée négociée, comme nouvel outil contractuel de protection comment tout doucement à voir le jour.

§2. Le recours à la vie privée négociée

La vie privée résulte d'un lien de droit puissant établi entre la personne et ses données personnelles. Le droit d'un individu sur ses données n'est pas un droit réel, c'est-à-dire sur une chose, mais un droit inhérent à l'individu. C'est pour cette raison qu'actuellement les données personnelles ne sont pas susceptibles de patrimonialisation (A). Cependant des aspirations à l'appropriation des données commencent à émerger (B).

A. L'actuelle non patrimonialisation des données personnelles

Etant donné que les données personnelles constituent des prolongements de la personnalité des individus, elles reflètent des éléments propres à l'individu comme l'identité, les choix personnels, le gabarit, etc.

C'est pourquoi depuis l'origine, la loi « Informatique et libertés » place le droit de la protection des données personnelles dans la catégorie de droits dits extrapatrimoniaux. En effet, les conceptions françaises et européennes font des informations personnelles des droits de la personnalité, c'est-à-dire des droits inhérents à la personne humaine. Le système étatsunien fait quant à lui primer, non pas l'intégrité de l'identité, mais l'aspect informationnel des données et leur exploitation commerciale.

Cette conception des données ne relève pas de l'évidence et cette difficulté tient au développement des procédés de communication⁴⁵⁷. Ces NTIC ont en effet permis de matérialiser des informations propres à l'individu sur des supports distincts facilement transmissibles. De même, bien que les droits de la personnalité soient normalement extrapatrimoniaux, une certaine forme de patrimonialisation a toujours existé, notamment lorsque le droit à l'image⁴⁵⁸, ou au nom⁴⁵⁹, peuvent faire l'objet de contrats d'exploitation et générer des revenus⁴⁶⁰.

Ce droit à la personne étant particulièrement consubstantiel à la personne, l'individu ne peut pas choisir d'en disposer librement de manière absolue. Etant des droits extrapatrimoniaux, ces droits ne relèvent donc pas de la qualification de bien et sont, par principe, hors du commerce. Ils sont alors incessibles, imprescriptibles et perpétuels.

⁴⁵⁷ R.LINDO, « Une création prétorienne : les droits de la personnalité », *Dalloz*, 1975, p. 11.

⁴⁵⁸ *Ibid.*

⁴⁵⁹ M.VIVANT, « Le patronyme saisi par le patrimoine », *Mélanges offerts à André Colomer, Litec*, 1993, p. 516.

⁴⁶⁰ T.REVET, « L'image de la personne est un bien », *RDT civ.*, 2009, p. 342.

Ainsi, le Conseil d'Etat rappelle-t-il qu'« en l'Etat du droit, il n'existe pas de droit de propriété de l'individu sur ses données personnelles. [...] la protection des données personnelles, telle qu'elle est conçue par la loi du 6 janvier 1978, la Convention n° 108 du Conseil de l'Europe ou la directive n° 95/46/CE, ne repose pas sur une logique patrimoniale, mais sur une logique de droits attachés à la personne [...] ; il n'existe pas de droit de propriété sur les données brutes »⁴⁶¹.

Ce choix de la qualification extrapatrimoniale des données a pour objectif de préserver l'intégrité de la personnalité en limitant leur utilisation commerciale. Or, le droit à l'autodétermination informationnelle telle que consacré par la loi du 7 octobre 2016 permet déjà à l'individu de contrôler ses données. La CNCDH rejoint cette idée. D'après elle, le droit à l'autodétermination informationnelle, qui fait partie intégrante des droits de la personnalité, reconnu par le Conseil d'Etat permet a priori de garantir le contrôle des données, cependant avec une plus grande souplesse⁴⁶².

Ces données reflétant la personne du citoyen il n'est pas en soi imaginable qu'elles puissent être évaluables en argent. La personne n'étant pas une chose, les données la concernant ne doivent pas l'être non plus. Cependant il s'avère que des aspirations à l'appropriation des données personnelles par les citoyens naissent, et ce dans le prétendu objectif de mieux contrôler l'utilisation de leurs données. Les « données personnelles relèveraient alors à la fois « de l'être et l'avoir »⁴⁶³.

B. Les aspirations à l'appropriation des données personnelles

Si la conception patrimoniale des données n'a pas été retenue, l'envisager n'est pas sans intérêt puisque qu'elle permettrait d'appréhender autrement la protection des données personnelles.

Dans la mesure où les droits à la vie privée et à la liberté dans la vie privée disparaissent progressivement au profit de logiques marchandes, le droit de propriété appliqué aux données permettrait de conférer aux individus un « droit réel sur leurs données afin de tenir en échec le droit d'autrui à l'information »⁴⁶⁴. Il faudrait alors repenser la protection des données

⁴⁶¹ CE, « Le numérique et les droits fondamentaux », *op. cit.*, p. 154

⁴⁶² Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *opt. cit.*

⁴⁶³ P.MOURON, « Pour ou contre la patrimonialité des données personnelles », *Revue Européenne des Médias et du Numérique*, n° 46-47, 2018, p.90.

⁴⁶⁴L.M AUGAGNEUR, *art., préc.*

personnelles au titre des catégorie de biens susceptible d'engendrer des contrats. La pénétration du droit civil dans le droit du travail retrouverait un second souffle.

Cette logique patrimoniale, issue du droit des contrats, n'est pas si insensée. Pour preuve, certaines dispositions du RGPD semblent s'en approcher.

Un rapprochement peut être fait avec le contrat de prêt à usage. Défini à l'article 1875 du Code civil, « le prêt à usage est un contrat par lequel l'une des parties livre une chose à l'autre pour s'en servir, à la charge par le preneur de la rendre après s'en être servi ». Or, dans le cadre de la relation de travail, le salarié livre certaines de ses données personnelles à l'employeur aux fins de l'activité de l'entreprise. Or, en confirmant ou consacrant des droits d'accès, d'opposition, d'effacement, de limitation de la durée de conservation et de portabilité des données personnelles, le RGPD instaure une sorte de contrat de prêt à usage dans lequel l'employeur doit rendre les données au bout d'un certain temps. Le salarié se trouve donc protégé contre toute « dépossession » de ses données personnelles.

Dès lors, l'idée d'instaurer un droit de propriété sur les données ne doit pas se réduire à une monétisation puisque tous les contrats de droit civil n'ont pas forcément une contrepartie financière en échange. En effet, comme l'a affirmé Valérie Peugeot, il ne faut pas oublier que le premier droit qui découlerait de la logique patrimoniale réside dans le droit de ne pas divulguer ses données⁴⁶⁵.

Le Think Tank libéral Génération libre, présidé par Gaspard Koenig, prône la thèse de la patrimonialisation des données personnelles⁴⁶⁶. Les arguments invoqués dans son rapport sont subtils. Il met en avant l'idée que l'instauration d'un droit de propriété privée sur les données n'aurait rien d'innovant puisque ces dernières ont déjà une valeur économique⁴⁶⁷, et donc peuvent être considérées comme des biens à part entière. De plus, les individus pourront négocier leur utilisation en se faisant éventuellement rémunérer en contrepartie. Ce droit permettrait ainsi de restaurer la souveraineté de l'individu sur son patrimoine informationnel⁴⁶⁸, et lui permettrait de profiter des bénéfices liés à leur utilisation. L'individu pourrait ainsi, tel David face à Goliath, tirer des bénéfices des géants du numérique en faisant fructifier ses données personnelles. Bien que séduisante, elle donne de prime abord au citoyen-salarié l'illusion de reprendre la main.

⁴⁶⁵ V. PEUGEOT, dans son billet : « Données personnelles: sortir des injonctions contradictoires », 2014.

⁴⁶⁶ Rapport 2018, « Mes data sont à moi – Pour une patrimonialité des données personnelles », Génération libre, janvier 2018.

⁴⁶⁷ P.STORRER, « Pour un droit commercial de l'exploitation des données à caractère personnel », *Recueil Dalloz*, 2013, p.844.

⁴⁶⁸ A.BENSOUSSAN, « Informatique et libertés », 2e éd., Francis Lefebvre, 2010, p. 42

Toutefois, il s'avère que la reconnaissance d'une propriété sur les données soit un leurre puisqu'elle n'apporte pas de réponse adéquate et présente de nombreux risques.

Tout d'abord, le renvoi de la protection des données sur l'individu déboucherait sur un « renforcement des inégalités entre citoyens numériques, entre ceux en capacité de gérer leurs données, de les protéger, les monétiser et ceux qui par manque de temps, ou toute autre raison, laisserait faire par défaut le marché »⁴⁶⁹. Apparaît alors le risque de voir naître l'idée d'une vie privée à négocier à double vitesse.

Ensuite, comme le souligne Irénée Régnard⁴⁷⁰, l'argumentaire tendant à considérer que se faire rémunérer pour ses propres données rend l'individu conscient et consentant quant à l'usage qui peut en être fait, est tronqué. En effet « revendre n'est pas maîtriser et responsabiliser l'individu ne le rend malheureusement pas automatiquement plus responsable »⁴⁷¹.

De plus, le concept de propriété heurte la conception de vie privée qui place sa protection notamment sur le terrain de la dignité humaine. Revendre ses données reviendrait alors à nier l'appartenance de l'homme à l'Humanité. En outre, le droit de propriété implique aussi le droit de céder la chose. Or il n'est pas possible de céder une donnée qui est un attribut de la personnalité de l'individu.

Aussi, instaurer un droit de propriété sur les données relatives à la vie publique (ou personnelle) du salarié reviendrait à remettre en cause la liberté d'expression.

Enfin, l'idée d'instaurer un droit de propriété ne ferait qu'aggraver le déséquilibre structurel entre les citoyens et les entreprises⁴⁷². En effet, s'il est possible de monnayer ses données personnelles, le contrat qui liera l'individu sera d'ordre commercial et « le petit David, que sont la majorité des individus, risque de se retrouver bien démuné pour se défendre quand il voudra se libérer des géants du Net. Il semble peu probable que cette fois, David l'emporte sur Goliath »⁴⁷³.

En tout état de cause, l'idée d'une rémunération en échange de ses données ne serait pas une avancée remarquable. En effet, d'une part une équivalence de cette rémunération existe déjà avec l'accès gratuit aux services numériques en échange des redoutables publicités⁴⁷⁴ et

⁴⁶⁹ V. PEUGEOT, *ibid.*

⁴⁷⁰ I.REGNAUD, *art., préc.*

⁴⁷¹ I.REGNAUD, *ibid.*

⁴⁷² N.OCHOA, « 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, p. 1157.

⁴⁷³ P.LATOMBE, « Patrimonialisation des données personnelles : la fausse bonne idée », *Médiapart*, 2019.

⁴⁷⁴ V.L BENABOU ET J.ROCHFELD, « A qui profite le clic ? Le partage de la valeur à l'ère numérique », *Odile Jacob*, 2015, p. 27.

d'autre part, individuellement les données n'ont que peu de valeur puisqu'elles ne commencent à avoir une véritable valeur économique que lorsqu'elles sont agrégées (« le big data »)⁴⁷⁵. Prises isolément, elles ne valent que quelques centimes d'euros, ce qui laisserait les individus dans l'espoir de pouvoir obtenir un revenu complémentaire.

Néanmoins, si cela venait à se produire, le triptyque usus, fructus, et abusus ne pourrait pas s'appliquer dans sa totalité puisque certains actes seraient par principe interdits. La patrimonialisation des données pourrait alors être exclue en raison du caractère sensible des données, comme celles touchant à la dignité des personnes⁴⁷⁶.

« La patrimonialité devra alors trouver les moyens de son organisation⁴⁷⁷ ».

Finalement, deux courants s'affrontent : les partisans de l'actuelle non patrimonialisation des données personnelles, et les défenseurs de sa patrimonialisation. La nature juridique des données personnelles ne fait donc que renouveler l'imprescriptible question du niveau de protection souhaitable. Quoiqu'il en soit, qu'il s'agisse de prééminence de la personnalité sur les intérêts économiques, ou de souveraineté de la personne sur ses biens, ces deux conceptions ont un objectif prétendument commun : la garantie d'une parfaite maîtrise de l'utilisation des individus sur leur données⁴⁷⁸.

CONCLUSION DU CHAPITRE II

La nature de la protection, à l'instar de la post-modernité qui innerve notre droit contemporain, se privatise, se flexibilise et se contractualise. En l'occurrence, la protection prend la forme de procédés a-juridiques et d'accords collectifs négociés, auxquels il appartiendra aux acteurs de la négociation collective de s'emparer. Il appartient aux acteurs de l'entreprise de créer un système où responsabilité rime avec compétence, ce qui fait cruellement défaut actuellement.

Au carrefour de la protection et de la liberté, le droit des données personnelles cherche un point d'équilibre que certains semblent voir dans la patrimonialisation des données. Toutefois, certains regards « tuent dans l'œuf » cette proposition.

⁴⁷⁵ S.MERCIER, dans son billet : « Biens communs et données personnelles : il nous faut inventer », 2014 : « Non ce qui est décisif, c'est le graphe, le croisement de ces données, les relations entre elles [...]. C'est l'interconnexion des données qui donne de la valeur à ces dernières ».

⁴⁷⁶ F.MATTATIA ET M.YAICHE, « Etre propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? », *Revue Lamy, Droit de l'immatériel*, n° 114, 2015, p. 60.

⁴⁷⁷ P.CATALA, « Le droit à l'épreuve du numérique – Jux ex Machina », Presses Universitaires de France, Collection 1137 Droit, Ethique, Société, Première édition, mai 1998, p. 228.

⁴⁷⁸ P.MOURON, *art., cit.*, p.90.

Dès lors, si la protection des données personnelles est particulièrement marquée par sa mutation, « l'arbre des mesures postmodernes qui accompagne ces changements les plus récents ne doit toutefois pas cacher la forêt qu'est la structure traditionnellement réglementaire de ce régime »⁴⁷⁹.

⁴⁷⁹ N.OCHOA, *op.,cit.*, p.267.

CONCLUSION PARTIE II

De protection, il n'est plus guère question à l'heure d'évoquer les objectifs de compétitivité des entreprises au sein de l'espace économique européen. L'uniformisation des législations afin de voir grandir les géants européens propres à combattre les champions d'autres horizons, semble plus à même de caractériser ce phénomène.

Arguons toutefois que constituer des champions européens, à la fois compétitifs et protecteurs des droits et libertés fondamentaux des citoyens-salariés peut constituer une bonne défense face à l'international. La protection ressurgira là où on ne l'attendait pas.

Ainsi, malgré le « marketing publicitaire » donné au RGPD en tant que nouvel instrument protecteur des données personnelles, il s'avère que, derrière ces belles paroles, se cache en réalité une volonté de placer l'Union européenne en tant que championne de l'économie numérique. Il s'agit alors d'un objectif économique très éloigné des intérêts du salarié puisqu'il ce qu'il en ressort n'est pas un objectif de protection individuelle mais un objectif de concurrence, d'adaptabilité et de flexibilité. Dès lors, la réglementation offre une protection en demi-teinte.

La protection des données personnelles des citoyens-salariés se met alors au service du marché. Dans un monde où l'ultralibéralisme s'impose, le législateur européen tente de créer un système cohérent au sein duquel la protection des citoyens-salariés, doit exister sans toutefois faire de l'ombre à la protection de la liberté du marché. Les mécanismes de protection s'en trouvent mutés. D'une réglementation a succédé la régulation, et des mécanismes de droit dur a succédé des mécanismes de droit mou. La protection des données personnelles se déjudiciarise et se sectorialise.

Le droit à la protection des données personnelles, droit extrapatrimonial par essence, se prend même à rêver de devenir un droit patrimonial dans lequel l'individu accepterait de négocier, par contrat, l'utilisation faite de ses données personnelles.

CONCLUSION GENERALE

Cette étude aura été l'occasion de mettre l'accent sur les conséquences du progrès numérique et technologique sur la préservation des droits et libertés fondamentaux des citoyens-salariés.

Si ces derniers sont susceptibles d'être bafoués par l'implantation de la technique dans l'entreprise, le RGPD renouvelle les moyens de protection des données personnelles des citoyens-salariés, en imposant la transformation de l'organisation voire même la transformation du modèle économique de la quasi-totalité des entreprises implantées sur le sol européen et/ou tractant les citoyens européens.

La protection des données personnelles des salariés a vu se produire des phénomènes nouveaux. Sa morphologie s'en est trouvée renouvelée. Au terme d'un changement de paradigme, l'influence toujours croissante de l'économique sur le social comporte des conséquences sur l'édifice du régime de protection.

Là où jadis prospéraient les mécanismes de formalités préalables, c'est désormais sur un mécanisme d'auto-contrôle et de responsabilisation des acteurs que fleurit l'effectivité des moyens de protection. Digne d'un slogan publicitaire trompeur, l'objectif de la refonte du régime de protection est en réalité un objectif de compétitivité et de croissance économique.

La question n'est alors plus de savoir quelle protection en Europe les décideurs souhaitent-ils construire. En l'occurrence, il est indéniable que la préférence est marquée du côté d'une Europe en priorité bienveillante envers ses champions (et futurs champions !) de l'économie numérique tout en s'assurant d'un discours d'une Europe davantage soucieuse des droits et libertés de ses citoyens-salariés européens.

Pareil constat ne peut toutefois faire l'économie de la nuance. Il doit être avancé que si une nouvelle étape – décisive ? – de décentralisation normative est franchie, les mécanismes de protection sont toujours d'actualité, même s'ils s'en trouvent transformés.

L'histoire moderne du droit de la protection des données personnelles est celle d'un droit plus conventionnel, davantage adapté à la réalité. Ce droit se veut pragmatique. C'est dans ce contexte que la libéralisation et la contractualisation des mécanismes de protection sont nées. Ces mécanismes ont su séduire au point de connaître un développement considérable jusqu'à supplanter les traditionnelles prescriptions réglementaires. La protection se veut

davantage sectorielle, à l'instar de la réglementation américaine. S'impose alors le constat de la complexité : la complexité d'une protection qui ne se veut pas uniforme pour l'intégralité des salariés, mais disparate en fonction des entreprises. Le prix de l'adaptabilité serait alors celui de la complexité que le nouveau droit des données personnelles ne s'est pourtant pas promis de juguler.

L'enjeu de notre pays sera alors se de montrer à la hauteur de ses espérances dans les années qui suivent, et ce, malgré l'adoption poreuse de sa nouvelle loi « Informatique et libertés » afin de montrer l'exemple d'une France à la fois compétitive et protectrice, malgré les doutes et les « coquilles » qui ont pu s'installer ces derniers temps. C'est peut-être en cela qu'elle retrouvera le cœur de ses citoyens-salariés tout en s'assurant de sa souveraineté numérique, future composante majeure de la souveraineté étatique⁴⁸⁰.

Ainsi, et pour conclure, si possible souverainement, toute cette analyse, « *chaque progrès donne un nouvel espoir, suspendu à la solution d'une nouvelle difficulté. Le dossier n'est jamais clos* »⁴⁸¹.

⁴⁸⁰ C.CASTETS-RENARD, *art., préc.*, p.29.

⁴⁸¹ C. LEVI-STRAUSS, « Le Cru et le cuit (Plon) », 1964.

BIBLIOGRAPHIE

I. OUVRAGES GENERAUX

GUINCHARD (S.) Et DEBARD (T.), « Lexique des termes juridiques », 21^e édition, 2014, Dalloz, p.68.

HUXLEY (A.), « Le meilleur des mondes », 1932, Pocket Jeunesse, Fantastisue, 2001. 285p.

MARX (K.), « Manuscrits de 1844 », Flammarion, 2006, 175 p.

ORWELL (G.), « 1984 », Trad. Par Amélie Audiberti, Gallimard, Paris, Folio 822. 438 p.

RAY (J-E.), « Droit du travail : droit vivant », 26^e éd., Wolters Kluwer, 2017.

ROUSSEAU (J-J.), « Du contrat social », Flammarion, 1992.

SUPIOT (A.), « La Gouvernance par les nombres », *Cours au Collège de France (2012-2014)*, Fayard, 2015.

TEYSSIE (B.), « Droit du travail, relations collectives », 11 éd., Lexisnexis, 2018.

THOREAU (H-D.), « La désobéissance civile », *Culture Commune*, 2014, p.1.

II. OUVRAGES SPECIAUX, THESES, MONOGRAPHIES

BENABOU (VL.) Et ROCHFELD (J.), « A qui profite le clic ? Le partage de la valeur à l'ère numérique », *Odile Jacob*, 2015, p. 27.

BENSOUSSAN (A.), *Informatique et libertés*, 2e éd., Francis Lefebvre, 2010.

BOURGEOIS (M.), *Droit de la donnée*, éd., Editions LexisNexit, 2017.

CARBONNIER (J.), « Droit civil », volume 1, Paris : PUF, 2004, p. 518

CODRON (C.), « La surveillance diffuse : entre Droit et Norme », Thèse Lille, 2018.

COUTURIER (G.), « Droit du travail. Les relations individuelles de travail », Paris, *PUF*, coll. : Droit fondamental, 3^{ème} éd., 1996.

DELVOLVE (V.), « La liberté d'entreprendre », Thèse, Paris II, 2002.

EL ATMANI (F.), « La protection des données personnelles dans l'Union européenne », Thèse de droit privé soutenue à la faculté de Montpellier, Septembre 1996, p.121.

EYNARD (J.), « Les données personnelles : quelle définition pour un régime de protection efficace », Paris, Michalon, 2013.

FEDAOUI (S.), « La protection des données personnelles face aux nouvelles exigences de sécurité », Mémoire Rouen, 2008.

GAILLARD (E.) « Le pouvoir en droit privé », Thèse, *Economica*, 1985.

DESGENS-PASANAU (G.) « La protection des données personnelles, le RGPD et la loi française du 20 juin 2018 », LexisNexis, 4^e édition, 2019.

LOKIEC (P.), « Il faut sauver le droit du travail ! », Odile Jacob, 2015, p. 17

OCHOA (N.), « Le droit des données personnelles, une police administrative spéciale », Thèse, Paris I, 2014.

PECAUT-RIVOLIER (L.), **STRUILLOU (Y.)**, **Et WAQUET (P.)**, « Le pouvoir de direction et les libertés des salariés », *LGDJ*, éditeur Liaisons, collection Droit vivant, 2014.

RIGAUX (F.), « La protection de la vie privée et les autres biens de la personnalité », *Bruylant LGDJ*, 1990.

TIMSIT (G.), « Archipel de la norme », *PUF*, 1997, p. 204

VITALIS (A.), « Pouvoir et Libertés », Paris, *Economica*, 1981, p.113.

III. ARTICLES.

ADAM (P.), « La dignité du salarié », *Rev. trav.* 2014, p.244

ASTAIX (A.), « Internet : une loi contre les atteintes à la vie privée », *D.* 2010, p.756

AUGAGNEUR (LM.), « Vers des nouveaux paradigmes du droit dans l'économie numérique », *RDT com.* 2015.

BARBIER-CHASSAING (F.), « Garantir la sécurité des données et mieux prendre en compte la cybercriminalité dans une logique de responsabilisation pour les entreprises », *Dalloz IP/IT* 2019, p.217.

BAREGE (A.) Et BOSSU (B.), « Les TIC et le contrôle de l'activité du salarié », *JCP S* n°41, 8 oct. 2013, p.1393.

BARRIERE (F.), « Les dispositifs d'alertes professionnelles : le temps de l'apaisement ? », *Rev. sociétés* 2011, p.276.

BLOUM (P.), « Le RGPD, révolution ou évolution », *Lextenso, Petites affiches – n°126*, 2018

BRUNET (A.), « Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation global », *Dalloz IP/IT*, 2016.

CADIO (P.) Et LIVENAIS (T.), « Photographie du champ territorial du règlement données personnelles : de nouveaux opérateurs concernés ? », *Dalloz IP/IT*, 2016.

CASTETS-RENARD (C.), « Les enjeux et l'actualité de la protection des données personnelles en Europe », « Quelles protections des données personnelles en Europe ? », *Larcier*, 2015

- « La protection des données personnelles dans les relations internes à l'Union européenne », *Dr.soc.* 2018 (actualisation : Mai 2019).
- « Brève analyse du règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p. 331.

CHAFIOL(F.) Et BARBET-MASSIN (A.), « La blockchain à l'heure de l'entrée en application du règlement général sur la protection des données », *Dalloz IP/IT*, 2017.

CHEVALLIER (J.), « De quelques usages du concept de régulation », in *MIAILLE Michel (dir.), La régulation entre droit et politique*, L'Harmattan, 1995, p.95

- « Vers un droit postmoderne ? », in *Les transformations de la régulation juridique*, dir.J. CLAM, G.MARTIN, *Droit et société* n°5, 1998, p.32.
- « Régulation et polycentrisme », *RA*, 1998, p.48.

CLUZEL-METAYER (L.) Et DEBAETS (E.), « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA*, 2018, p.1101.

DEBET (A.), « Les nouveaux instruments de conformité », *Dalloz IP/IT*, 2016, p.592.

DEPREZ (J.) « La Cour de cassation », in *Les transformations du droit du travail, Etudes offertes à Gérard Lyon-Caen*, Dalloz, 1989, p.171.

DESGENS-PASANAU (G.), « Formation et sensibilisation des nouveaux acteurs : quelles solutions ? », *JA* 2018, n°571, p.27

- « RGPD : entre incertitudes et occasions manquées », *Dalloz IP/IT*, 2016, p. 335

- DE TISSOT (O.),** « La protection de la vie privée du salarié », *Dr.soc.*, 1995, p. 222
- DOUVILLE (T.),** « Blockchain et protection des données à caractère personnel », *AJ contrat* 2019, p. 316
- DUEZ-RUFF (V.),** « Impact des nouvelles technologies sur le droit du travail : un salarié appartient-il virtuellement à son employeur ? », *Lexbase Hebdo* éd. Soc. n°498, 2012.
- ESCANDE-VARNIOL (MC.),** « Un ancrage stable dans un droit du travail en mutation », *D.* 2019, p.77.
- FAVENNEC-HERY (F.),** « Vie professionnelle, vie personnelle du salarié et droit probatoire », *Dr.soc.* 2004, p. 48.
- K. FAVRO,** « La CNIL, une autorité à "l'âge de la maturité" », *Dalloz IP/IT*, 2018, p.464.
- FRAYSSINET (J.),** « Nouvelles technologies et protection des libertés dans l'entreprise », *Dr.soc.* 1992, p.596.
- **Et P.KAYSER,** « La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le décret du 17 juillet 1978 », *RDP*, 1979, p. 632
- GAMET (L.),** « Biométrie et travail », *Dr.soc* 2019, p. 422
- HAAS (G.),** « Bilan après neuf mois d'application du RGPD », *Dalloz IP/IT*, 2019, p.357
- HUET-WEILLER (D.),** « La protection juridique de la voix humaine », *RTD civ.* 1982, p. 497.
- JANUEL (P.),** « CNIL et RGPD : retour sur une année de transition », *Dalloz actualité.*, 19 avril 2019
- JAULT-SESEKE (F.) Et ZOLYNSKI (Z.),** « Le règlement 2016/679/UE relatif aux données personnelles, *ADIP*, 2016, p. 1877.
- LANG (G.),** « Vocabulaire de la statistique et de la protection juridique des données individuelles », *Courrier des statistiques*, n° 107, 2003
- LECOURT (A.),** « RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises », *Dalloz IP/IT* 2019, p.205
- LENOIR (N.) ; DILL (A.) Et BERION (H.),** « Lanceurs d'alerte - Alerte professionnelle et protection des données personnelles », *La Semaine Juridique Edition Générale* n° 19-20, 7 Mai 2018, doct. 553.

LESAULNIER (F.), « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016, p.573.

LINDO (R.), « Une création prétorienne : les droits de la personnalité », *Dalloz*, 1975, p. 11.

LOISEAU (G.), « Des droits patrimoniaux de la personnalité en droit français », *Rev. dr. McGill*, juin 1997, p. 319 et s.

- « Typologie des choses hors du commerce », *RTD civ*, 2000, p. 46.
- « Focus sur la vie personnelle du salarié », *D.* 2009, p.2393
- « Your employer is watching you », *Cah.soc.*, 2013, n°255, p : 333
- **Et MARTINON (A.)**, « L’Homo Numericus », *Les Cahiers Sociaux*, n°290, p.519
- « Droit civil et droit du travail : une relation instable », *Dr.soc.*2019, p.477.

LYON-CAEN (A.) Et VACARIE (I.), « Droits fondamentaux et droit du travail », *Mélanges en l’honneur de J. M. Verdier*, *Dalloz*, 2001, p. 421.

MAISANI (P.) Et WIENER (F.), « Réflexions autour de la conception post-moderne du droit », *Droit et société*, n° 27, 1994, p. 443.

MARTIAL-BRAZ (N.), « Le renforcement des droits de la personne concernée », *Dalloz IP/IT* 2017, p.253

METALLINOS (N.), « La fonction de « détaché à la protection des données » en Allemagne et aux Pays-Bas », *Dr.soc*, 2004, p.1066.

- **Et DEBET (A.)**, **MASSOT (J.)**, « Informatique et libertés. La protection des données à caractère personnel en droit français et européen », *Lextenso*, coll. « Les intégrales », 2015, spéc.n°379 et s.
- « Les apports du règlement général relatif à la protection des données personnelles sur les conditions de licéité des traitements », *Dalloz IP.IT*, 2016, p.588.

MOULY (J.) Et SAVATIER (J.), « Droit disciplinaire – Fautes disciplinaires », *RDT*, 2019.

MOURON (P.), « Pour ou contre la patrimonialité des données personnelles », *Revue Européenne des Médias et du Numérique*, n° 46-47, 2018, p.90.

NAFTALSKI (F.), « L’impact du nouveau règlement sur les stratégies de transferts internationaux de données personnelles », *Dalloz IP/IT*, 2016, p.340.

PECAUT-RIVOLIER (L.), **STRUILLOU (Y.)**, **et WAQUET (P.)**, « Le pouvoir de direction et les libertés des salariés », *LGDJ*, éditeur Liaisons, collection Droit vivant, 2014

PELLET (S.), « RGPD : l’effacement du consentement », *Revue générale du droit des assurances* - n°01 – p.6.

PERRAY (R.), « La délimitation territoriale du RGPD : le champ d'application et les transferts de données hors de l'Union européenne », *Dalloz IP/IT*, 2016, p. 581.

PEYRONNET (M.), « La vie privée du salarié sur internet en voie d'extinction », *Dalloz actualités*, 29 janvier 2016

POUSSON-PETIT (J.), « L'identité de la personne humaine », *Etude de droit français et de droit comparé*, Bruylant, 2002.

RAY (JE.), « A propos de la révolution numérique », *Dr.soc*, 2012, p.934

RICHARD DE LA TOUR (J.), « La vie personnelle du salarié. Étude sur la jurisprudence récente de la chambre sociale de la Cour de cassation », Rapport annuel de la Cour de cassation pour l'année 1999.

SAURON (JL.), « Le RGPD : outil ou entrave de la société d'information ? », *Dalloz IP/IT*, 2016 p.17

SCHULTIS (C.), « Le traitement de données dans le cadre des relations de travail dans le règlement sur la protection des données personnelles », *Dalloz IP/IT*, 2017, p. 265.

SCHWARTZ (J.), « Le point sur le RGPD : nouvelles obligations, nouveaux enjeux », *Les Cahiers Sociaux* –n°306, p.228.

STORRER (P.), « Pour un droit commercial de l'exploitation des données à caractère personnel », *Recueil Dalloz*, 2013, p.844.

STROWEL (A.), « Quelles protections des données personnelles en Europe ? », *Larcier*, 2015

SUPIOT (A.), « Travail, droit et technique », *Dr.soc*, 2002, p.13.

- « Fragments d'une politique législative du travail », *Dr.soc*, 2011, p.1151.

TAMBOU (O.), « L'introduction de la certification dans le RGPD : quelle valeur ajoutée ? », *RLDI*, 2016, n°3969, p.43.

TESTARD (C.), « Le droit souple, une « petite » source canalisée », *AJDA* 2019, p. 934.

TEYSSIE (B.), « Droit du travail et droit des affaires », *D.* 2004, p. 2698

VIVANT (M.), « Le patronyme saisi par le patrimoine », *Mélanges offerts à André Colomer, Litec*, 1993, p. 516.

- **Et MALLET-POUJOL (N.),** « Informatique », Répertoire de droit international, janvier 2019.

WAQUET (P.), « La vie personnelle du salarié », *Dr.soc*, 2004, p.23

- « Vie privée, vie professionnelle et vie personnelle », *Dr.soc.*, 2010, p.14.

WILLMANN (C.), « Esclavage – Travail forcé – Traite des êtres humains », Répertoire de droit pénal et de procédure pénale, octobre 2006 (actualisation : janvier 2017)

ZOLYNSKI (C.), « Les nouveaux contours de l'action de groupe et de l'action collective au lendemain de la loi pour la protection des données : un empowerment renforcé », *Dalloz IP/IT* 2018, p.470.

IV. AVIS, RAPPORTS

- CE, « Le numérique et les droits fondamentaux », La Documentation Française, 2014, p. 177-178 ;
- Avis du G29, 15/2011 du 13 juill.2011 sur la définition du consentement, WP 187, p.15 ; v. égal. L'avis du G29, WP 48 sur le traitement des données à caractère personnel dans le contexte professionnel ;
- [Communiqué G29] Séance plénière du G29 des 12 et 13 décembre 2016 ;
- CE, avis, 7 déc. 2017, n° 393836 ;
- Rapport CNIL, déc 2017, « comment permettre à l'homme de garder la main ? – Les enjeux éthiques des algorithmes et de l'intelligence artificielle » ;
- CNCDH, avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, JORF n°0126 du 3 juin 2018 texte n° 63.

V. Sites Internet, publications

BOUCHER (P.), « SAFARI ou la chasse aux Français », *Le Monde*, 21 mars 1974.

KOENIG (G.), « Mes data sont à moi – Pour une patrimonialité des données personnelles », Génération libre, Rapport janvier 2018.

MERCIER (S.) « Biens communs et données personnelles : il nous faut inventer », Blog, 2014.

MILLET (S.), « La protection des données personnelles en chantier : le RGPD vu sous l'angle des données RH », *Cabinet ELLIPSE Avocat*, 2018.

NAILLAT (S.), « La blockchain, un risque pour les données personnelles ? », *in La Tribune*, 2018.

PEUGEOT (V.), Données personnelles: sortir des injonctions contradictoires », *VECAM*, 2014.

- « RGPD : quelle place pour l'action collective ? », *VECAM*, 2018.

REES (M.), « Le RGPD expliqué ligne par ligne », *Blog*, 2018.

REGNAUD (I.), « Mais où va le web », in « Revendre ses données personnelles, la fausse bonne idée », *Blog*, 2018.

ROCHFELD (J.), « l'action de groupe est-elle vraiment collective ? » *VECAM*, 2018.

VI. DELIBERATIONS CNIL

- CNIL, recom., n°83-058., 29 nov. 1983 ;
- CNIL, délib., n° 2005-110 et n° 2005-111, 26 mai 2005 ;
- CNIL, délib. n°2009-474., 23 juillet 2009 ;
- CNIL, délib.n°2010-112., 22 avr.2010 ;
- CNIL délib n°2014-307., 17 juillet 2014 ;
- CNIL délib., n°2017-009., 15 juin 2017 ;
- CNIL, délib., n° 2017-191., 22 juin 2017 ;
- CNIL, délib. n° 2017-095., 23 mars 2017 ;
- CNIL, délib. n°2017-220.,13 juillet 2017 ;
- CNIL, délib n° 2017-299.,30 novembre 2017 ;
- CNIL, délib. n° 2018-042., 8 février 2018 ;
- CNIL, 29 nov. 1983 n°83-058 : recommandation NIR

VII. REREFERENCE NORMATIVE

1) Décisions constitutionnelles

- Cons.const.16 janv.1982,n°81-132 DC ;

- Cons.const.,20 juillet 1988, n°88-244 DC ;
- Cons.const., 23 juill. 1999, n°99-416, DC, JO 28 juill.1999 ;
- Cons. const., 12 juin 2018, n° 2018-765 DC, Loi relative à la protection des données personnelles, *AJDA* 2018. 1191.

2) Textes de valeur législative et règlementaire

- Loi n°70-643 du 17 juillet 1970, JORF 19 juillet 1970 ;
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF 7 janvier 1978, p. 227 ;
- 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 et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO 7 août 2004, p. 14063 ;
- Loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations ;
- Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, JORF n°75 du 29 mars 2014, p. 6123 ;
- Loi n° 2016-1321 du 7 oct. 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016 ;
- Loi n° 2016-1547 du 18 nov. 2016 de modernisation de la justice du XXI^e siècle, JORF n°0269 du 19 novembre 2016 ;
- Décret n°2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise ;
- Loi dite « Sapin II » n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, JORF n°0287 du 10 décembre 2016 ;
- Décret n° 2017-564 du 19 avril 2017 relatif aux procédures de recueil des signalements émis par les lanceurs d'alerte, JORF n°0093 du 20 avril 2017, applicable depuis le 1er janvier 2018 ;
- Loi n°2018-493, 20 juin 2018 relative à la protection des données personnelles, JORF n°0141 du 21 juin 2018 ;

- Décret n°2018-687 du 1^{er} août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF n°0288 du 13 décembre 2018 ;
- Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire, JORF du 21 avril 2019.

3) Textes internationaux et européens

- Dir. 95/46/CE 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, 24 oct. 1995, JOCE du 23 nov. 1995 ;
- BUREAU INTERNATIONAL DU TRAVAIL, Protection des données personnelles des travailleurs, Recueil de directives pratiques du BIT, Organisation internationale du travail, 1997, 52 p ;
- Communication de la Commission au Parlement européen, au conseil, au comité économique et social européen et 1062 au comité des régions, Com (2017) 9 final, « Créer une économie européenne fondée sur les données », Bruxelles, 2017 ;
- Régl.n°(UE) 2016/679 du Parlement européen et du Conseil, 27 avr.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.

4) Décisions des juridictions administratives

- CE.,6 novembre 2009, n°304300 ;
- CE.,12 mars 2014, n°353193 ;
- CE, 18 novembre 2015, n°371196 ;
- CE, 8 février 2017, 10ème - 9ème Chambres réunies, n° 393714 ;
- CE. 15 décembre 2017, n°403776.

5) Décisions des juridictions judiciaires

- Cass. soc. 17 Mai 1982 n° 80-16.541 ;
- Cass., 1re Civ. 23 octobre 1990, n° 89-13.163 ;
- Cass.soc.; 20 novembre 1991, n°88-43.120 ;
- Cass. soc. 9 décembre 1992 n° 89-42.547 ;
- Cass.soc; 22 mai 1995, n°93-44.078 ;
- Cass. soc. 14 Mai 1997 n° 94-45.473 ;
- Cass.soc., 21 juin 2000, n°98-41585 ;
- Cass.soc., 2 oct.2001, n°99-42-942 ;
- Cass.soc 7 juin 2006, n°04-43.866 ;
- Cass. soc., 18 oct. 2006, n°04-48.025 ;
- Cass.soc 30 mai 2007, n°05-43.102 ;
- Cass.soc., 10 juin 2008, n°06-16.229 ;
- Cass.soc., 9 juillet 2008, n°06-42.800 ;
- Cass.soc., 17 juin 2009, n°08-40274 ;
- Cass.soc 3 novembre 2011 n°10-18.036 ;
- Cass. soc., 26 juin 2012, n°11-15.310 ;
- Cass. soc. 4 juillet 2012, n°11-12330 ;
- Cass. soc., 12 février 2013, n°11-28.649 ;
- Cass. soc., 19 juin 2013, n°12-12.138 ;
- Cass.soc; 26 juin 2013, n°12-16.564 ;
- Cass.soc 17 décembre 2014, n°13-23645 ;

- Cass.soc., 30 juin 2016, n°15-10.557 ;
- Cass, 1ère ch. civ., 3 novembre 2016, n°15-22.595 ;
- Cass.soc 18 janvier 2018 n°16-20.618.

6) Décisions des juridictions européennes

- CEDH, Pretty c/ Royaume-Uni, 29 avril 2002, req. n°2346/02 ;
- CEDH, Christine Goodwin c/ Royaume-Uni, Grande chambre, 11 juillet 2002, req. n° 28957/95 ;
- CJUE « Österreichischer Rundfunk » du 20 mai 2003, e.a., C-465/00, C-138/01 et C-139/01 ;
- CEDH, 19 septembre 2013, Von Hannover c/Allemagne, n°8772/10, CEDH 2013 ;
- CJUE, 13 mai 2014, Google Spain, aff. C-131/12, JurisData n°2014-009597 ;
- CJUE 6 oct.2015, aff. C-362/14, Schrems c/Data Protection Commissioner ;
- CJUE, 19 oct. 2016, Patrick Breyer c/ Bundesrepublik Deutschland, aff. C-582/14, D. 2016. 2215 ;
- CEDH, 22 février 2018, requête n°588/13, Aff. Libert c. France.

TABLE DES MATIERES

Sommaire	4
Liste des abréviations	6
Introduction générale	9
1^{ère} partie – L’incidence de la protection des données personnelles sur la relation de travail	22
Chapitre I – L’enjeu de la protection	23
Section 1 – L’assimilation de la protection à la protection de la vie privée du salarié.....	23
§1 – L’évolution de la vie privée à l’âge de l’ « homo sapiens »	23
A) La protection traditionnelle au cercle intime du salarié	24
B) La protection extensive au cercle personnel du salarié	26
§2 – La transformation de la vie privée à l’âge de l’ « homo numericus ».....	28
A) La protection du droit à l’autodétermination décisionnelle du salarié	29
B) La protection du droit à l’autodétermination informationnelle du salarié	31
Section 2 – La non-réductibilité de la protection à la protection de la vie privée du salarié ...	33
§1 – La protection des données personnelles comme garante de la dignité	33
A) La garantie contre la discrimination	34
B) La garantie contre l’objectivation	37
§2 –La protection des données personnelles comme rempart au pouvoir de l’employeur ...	40
A) La garantie contre l’arbitraire de l’employeur	40
B) La garantie contre l’opacité de l’entreprise	41
Conclusion du chapitre I	44
Chapitre II – Les moyens de la protection	46
Section 1 – L’examen de la licéité	46
§1 – La licéité par l’existence de principes liés à la collecte	46
A) L’importance de la nature des données collectées.....	46

B) L'importance de la qualité des données collectées	49
§2 – La licéité par l'existence de principes liés au traitement des données	51
A) L'anéantissement du traitement avec consentement	51
B) Le renforcement des règles d'intelligibilité du traitement	54
Section 2 – L'examen de l'effectivité	56
§1 –La modernisation de la maîtrise des données transmises.....	56
A) La confirmation des droits existants	56
B) La consécration de nouveaux droits	59
§2 –L'adaptation des garants de la protection des données	61
A) Le responsable de traitement comme gardien du régime de protection	61
B) La CNIL comme clef de voûte du régime de protection	64
Conclusion du chapitre II	67
Conclusion 1 ^{ière} partie	68
2^{ème} partie – L'incidence du droit des données personnelles sur la protection des données personnelles des salariés	70
Chapitre 1 – La consécration du droit des données personnelles, source de retrait des mécanismes de protection	71
Section 1- La protection comme exception à la liberté d'entreprendre de l'employeur	71
§1 – La liberté de traitement comme composante de la liberté d'entreprendre	71
A) Le principe de la liberté de traitement	71
B) Les restrictions à la liberté de traitement	74
§2 – La liberté de sous-traitance comme composante de la liberté d'entreprendre	76
A) La consécration d'une responsabilité conjointe	76
B) L'affirmation d'une responsabilité ménagée	79
Section 2 – La protection comme exception à l'objectif de renforcement du Marché intérieur	81
§1 –La protection comme entrave à la compétitivité des entreprises	81
A) Une uniformisation nécessaire pour favoriser la concurrence.....	81
B) Une uniformisation partiellement atteinte	83

§2 –La protection à l’épreuve de l’internationalisation des flux transfrontaliers	85
A) Une extension du champ d’application territorial en raison de la déterritorialisation...85	
B) Une extension du champ d’application en raison des transferts hors Union européenne	87
.....	
Conclusion chapitre I	90
Chapitre 2 – La mise en œuvre du droit des données personnelles, source de mutation des mécanismes de protection	92
Section 1 - La libéralisation des mécanismes de protection	92
§1 – La mutation de la nature des mécanismes de protection : de la réglementation à la régulation.....	93
A) La réduction du droit à une régulation par les entreprises	93
B) La réduction du droit à une régulation par les technologies	95
§2 –La mutation de la juridicité des mécanismes de protection	96
A) La privatisation des mécanismes de contrôle	97
1) La privatisation par les procédures de contrôle interne	98
2) La privatisation par les actions de sensibilisation et de formation	99
B) Les procédés extra-juridiques des mécanismes de protection	101
Section 2 - La contractualisation des mécanismes de protection	104
§1 –Le recours au droit négocié	104
A) La déjudiciarisation de la défense des intérêts collectifs	104
1) Le recours à la négociation collective	104
2) Le recours aux chartes d’entreprises	106
B) La réinjection de moyens d’actions collectifs	107
1) Le recours aux actions de groupe	108
2) Le recours aux actions syndicales	109
§2 –Le recours à la vie privée négocié	110
A) L’actuel non-patrimonialisation des données personnelles	110
B) Les aspirations à l’appropriation des données personnelles	111
Conclusion du Chapitre II	114

Conclusion 2 ^{ième} partie	116
Conclusion générale	117
Bibliographie	119
Table des matières	131