FACULTÉ DES SCIENCES JURIDIQUES POLITIQUES ET SOCIALES

MARINE MAIKUCHEL

MASTER 2 DROIT DES AFFAIRES PARCOURS PROPRIETE INDUSTRIELLE

MÉMOIRE – SOUS LA DIRECTION DE MADAME BLARY- CLEMENT

PROFESSEURE ET RESPONSABLE DU MASTER 2 PROPRIÉTÉ INDUSTRIELLE

E-COMMERCE ET PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL :

Vers un renforcement de la protection des données à caractère personnel des consommateurs dans le cadre des opérations de e-commerce

Comment le règlement européen 2016/679 concrétise-il le renforcement de la protection des consommateurs à l'égard du traitement de leurs données à caractère personnel, en tant que personnes concernées par un traitement à des fins commerciales sur internet ?

SEPTEMBRE 2017

REMERCIEMENTS

Je remercie Madame Edith Blary-Clément, pour avoir assuré le suivi de mon travail et pour ses prompts conseils m'ayant permis de trouver des solutions pour avancer dans la réalisation du mémoire.

Ensuite, Je remercie l'ensemble de l'équipe de l'entreprise ZTP SERVICES, pour m'avoir permis d'appréhender la nouvelle règlementation européenne sur les données à caractère personnel de manière pratique.

Je remercie également Nicolas Duquesne, juriste technologies de l'information pour sa connaissance, sa disponibilité et son esprit critique sur le sujet des données à caractère personnel.

Enfin, je remercie Sabine Duez et Virginie Sacchi, juristes propriété intellectuelle, pour leur ouverture d'esprit et leur intérêt pour la problématique des données à caractère personnel.

SOMMAIRE

Liste des principales abréviations ……..... p. 3
Introduction …….. p. 4

PREMIERE PARTIE
LE RENFORCEMENT DES OBLIGATIONS DE L'E-COMMERCANT

Chapitre I – La mise en place d'une stratégie de gouvernance des données …… p. 9
Chapitre II – L'analyse des risques du traitement sur la vie privée ……. p. 23

DEUXIEME PARTIE
LE RENFORCEMENT DES DROITS DES CONSOMMATEURS

Chapitre I – Le renforcement des droits préalablement à la collecte ……... p. 41
Chapitre II – Le renforcement des droits postérieurement à la collecte …….. p. 56

Conclusion ……... p. 69
Bibliographie ……... p. 71
Table des matières …… p. 77

LISTE DES PRINCIPALES ABREVIATIONS

Art.	Article
CA	Cour d'appel
CCE	Communication, Commerce électronique
C. consom.	Code de la consommation
CE	Conseil d'Etat
CJUE	Cour de justice de l'Union européenne
CNIL	Commission Nationale de l'Information et des Libertés
Consid.	Considérant
C. post. Comm. Électr.	Code des postes et des communications électroniques
D.	Dalloz (recueil)
FEVAD	Fédération E-commerce et Vente à distance
JCP G	Semaine Juridique, Edition Générale
LCEN	Loi pour la confiance dans l'économie numérique
RDBF	Revue Droit bancaire et financier
R.UE	Revue de l'Union européenne
RGPD	Règlement général sur la protection des données
RLDI	Revue Lamy Droit de l'immatériel

INTRODUCTION

1 Le e-commerce, ou commerce électronique, reçoit une définition légale. Celui-ci peut se définir comme « *l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services* »[1]. Cette forme de commerce ne cesse de croitre comme l'attestent les différentes études de la Fédération E-commerce et Vente À Distance (FEVAD) effectuées chaque année[2].

2 Le e-commerçant, qui est donc la personne assurant par voie électronique la vente de biens ou de services, remplit la fonction d'éditeur de site, à l'occasion de cette activité économique. En effet, l'e-commerçant par le biais de son site a pour activité « *d'éditer un service de communication au public en ligne* »[3]. L'e-commerçant est donc astreint aux différentes obligations de l'éditeur de site[4]. Là ne s'arrête pas l'activité du e-commerçant.

3 Par le biais d'un site d'e-commerce, les consommateurs désirant bénéficier d'un bien ou d'un service sont amenés à renseigner des données les concernant. Le renseignement des données peut s'opérer de manière directe, lorsque le consommateur communique, par exemple, ses noms, prénoms et adresse nécessaires à la création d'un compte client ou à la livraison d'un bien. L'information des données peut également s'opérer de manière plus indirecte, voire à l'insu du consommateur, par le placement de traceurs sur l'ordinateur du consommateur[5].

4 La majorité de ces données remplissent la définition de « données à caractère personnel », énoncée par la Loi informatique et liberté[6] en son article 2. L'article dispose que « *constitue une donnée à caractère personnel toute information relative à une personne*

[1]L. 21 juin 2004, art. 14, dite LCEN

[2] Notamment le dernier bilan en date montre que les Français ont dépensé 72 milliard d'euros sur internet en 2016, v. notamment : M. Vivant, « Bilan 2016 du e-commerce en France : le cap des 70 milliards a été franchi », *RLDI* n°134, 1e fev. 2017

[3] LCEN, art. 6-1° I

[4]Sur les problématiques relatives à la qualification d'éditeur de site ou d'hébergeur v. CA Paris, pôle 5, 1re ch., 14 avril 2010, RLDI 2010/62, n°2034 : « l*a LCEN distingue au sein des services de communication au public en ligne entre le service d'hébergeur qui répond à la définition (…) de l'article 6-I-2 d'où il résulte que sera tenu comme tel le prestataire technique qui met à disposition du public le stockage de contenus fournis par des destinataires de ce service et le service éditeur, qui a le pouvoir de déterminer les contenus mis à la disposition du public en sorte que le critère du partage ainsi opéré réside dans la capacité d'action du service sur les contenus mis en ligne* ».

[5]Les données peuvent en effet être collectés par le biais de « cookies » ; v. infra point n°68 et suivants

[6]L. 6 janvier 1978, dite Loi Informatique et Libertés

physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». La présence de données à caractère personnel entraine l'application du régime protecteur prévu par la loi, lorsque celles-ci subissent un traitement, défini au même article comme « *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 […]* ».

5 Le e-commerçant, dans la gestion de son activité économique et de son site, entre donc en possession de différentes données à caractère personnel de ses clients et, plus généralement, de tout consommateur se rendant sur son site. Il peut être amené à traiter leurs données, en les enregistrant ou en les conservant par exemple. Le e-commerçant remplit donc la fonction de responsable du traitement définie comme la personne qui détermine les finalités et moyens du traitement des données[7].

6 En tant que responsable du traitement, l'e-commerçant est astreint aux obligations prévues par le Chapitre V de la Loi informatique et libertés. Celui-ci est également tenu de prendre en compte les recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL)[8]. Le respect de la réglementation relative au traitement des données à caractère personnel est placé sous le contrôle de la CNIL qui dispose de prérogatives afin de contraindre les responsables du traitement au respect des dispositions de la loi[9]. La CNIL se révèle être un garant efficace du respect de la protection des données à caractère personnel des personnes concernées par le traitement dans le secteur du commerce électronique[10].

7 L'évolution constante des technologies et l'augmentation des volumes de données collectées ont conduit le législateur européen à harmoniser et adapter la réglementation relative aux données à caractère personnel ; ce afin d'assurer une meilleure protection des données des

[7]L. 6 janvier 1978, art. 3

[8]Les principales recommandations intéressant l'e-commerçant étant :
(1) Délibération n°2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et autres traceurs visés à l'article 32-II de la loi du 6 janvier 1978 ;
(2) Délibération n°2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et prospects

[9]La CNIL dispose ainsi de la possibilité d'adresser des avertissements publics, des mises en demeure et de prononcer des sanctions administratives à l'encontre d'un responsable du traitement contrevenant à la loi.

[10]Pour exemple, la CNIL a délivré un avertissement et une mise en demeure publique à CDISCOUNT en raison de manquements graves portant notamment sur la sécurité des données : Délibération n°2016-265 du 20 septembre 2016

citoyens européens. La Directive n°95/46/CE du 24 octobre 1995, qui régit jusqu'à présent la protection des données à caractère personnel, lie les Etats membres destinataires quant au résultat à atteindre mais laisse aux instances nationales la compétence quant à la forme et aux moyens[11]. Du fait de la transposition de cette instrument communautaire, une disparité des législations en matière de protection des personnes physiques à l'égard de leurs données à caractère personnel s'est développée. Le constat de Fabrice Mattatia ne peut être contesté : « l*a Directive a engendré, par transposition, 27 droits nationaux des données personnelles dont la prise en compte constitue une charge pour les entreprises transeuropéennes qui doivent par exemple gérer 27 régimes de formalités différentes* »[12]. La commission a ainsi souhaité remplacer la directive par un règlement, directement applicable et permettant une homogénéisation de la législation relative aux données à caractère personnel au sein de l'Union européenne.

8 Après quatre années de négociation, le Parlement européen a définitivement adopté, le 14 avril 2016, la nouvelle législation européenne sur la protection des données à caractère personnel : le Règlement n°2016/679 du Parlement européen et du Conseil du 27 avril 2016[13], relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE. Ses dispositions seront directement applicables dans tous les Etats membres à partir du 25 mai 2018. L'ambition de ce nouvel outils réglementaire est double :

- Mettre à jour le dispositif de la Directive CE/95/46 afin de l'adapter aux évolutions survenues depuis lors[14] ;
- D'uniformiser les règles de protection des données personnelles dans l'Union européenne.

9 Une mise en conformité avec cette nouvelle législation par l'e-commerçant dans son activité de traitement de données est à opérer dès aujourd'hui. Aussi, l'adoption d'un outil règlementaire contraignant et d'application directe conforte le fait que la protection des personnes physiques à l'égard des données à caractère personnel est une priorité et tend à vouloir

[11] Conformément à l'article 288 du Traité du fonctionnement de l'Union Européenne (TFUE)
[12] F. Mattatia, *Le droit des données personnelles : n'attendez pas que la Cnil ou les pirates vous tombent dessus*, Eyrolles, 2e Ed., 2016, p. 215
[13] Ci-après « le Règlement » dans le corps du mémoire
[14] Notamment aux évolutions liées à l'explosion d'internet, des objets connectés, du cloud computing, etc.

être renforcée.

10 **Mais encore faut-il s'interroger sur la manière dont le Règlement concrétise le renforcement de la protection des consommateurs à l'égard de leurs données à caractère personnel, en tant que personnes concernées par un traitement à des fins commerciales sur internet.**

11 Le rehaussement de protection des consommateurs relativement à leurs données à caractère personnel se matérialise de manière indirecte, par un renforcement des obligations du e-commerçant en tant que responsable du traitement (**Partie I**). Plus directement, le renforcement des droits des consommateurs, en tant que personnes concernées par le traitement, parachève cette consolidation de protection des données les concernant (**Partie II**).

PARTIE I : LE RENFORCEMENT DES OBLIGATIONS DE L'E-COMMERCANT

12 Le Règlement 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 alourdit les obligations à la charge du responsable du traitement[15] ; procédant à un renforcement indirect de la protection des données à caractère personnel des consommateurs dans le cadre d'une opération d'e-commerce. En effet, le règlement renforce les obligations de ceux qui effectuent ou déterminent le traitement des données à caractère personnel, responsables de traitements et sous-traitants.

13 Tout traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union européenne doit être effectué conformément aux principes édictés par le Règlement, que le traitement lui-même ait lieu ou non dans l'Union européenne[16].

14 Le Règlement européen innove quant à l'obligation pour le responsable du traitement de protéger les données. Le texte incite le responsable du traitement à la mise en place d'une stratégie de gouvernance des données (**Chapitre I**). Aussi, une approche par les risques du traitement, imposé par le règlement, implique de nouvelles obligations à la charge du responsable du traitement, assurant ainsi un rehaussement de la protection des personnes concernées par le traitement (**Chapitre II**).

[15] Un Chapitre entier est ainsi consacré à ses obligations : RGPD, Chapitre V « *Responsable du traitement et sous-traitant* »

[16] RGPD, art. 3 sur le champ d'application territorial du Règlement

CHAPITRE I : LA MISE EN PLACE D'UNE STRATEGIE DE GOUVERNANCE DES DONNEES

15 Le règlement entend responsabiliser le responsable du traitement en lui imposant d'être en mesure de démontrer, en cas de contrôle, qu'il est conforme à la réglementation : cela est le principe d'*accountability*, consacré par le règlement européen[17] (**Section I**). Une des conséquences impliquées par la responsabilisation de l'entreprise est l'obligation de protéger les données dès la conception et par défaut (**Section II**). Cette responsabilisation et l'obligation de protéger les données en amont des projets contraignent le responsable du traitement à l'adoption d'une culture de la donnée, et ainsi à la mise en place d'une stratégie de gouvernance des données.

SECTION I - Le respect du principe d'accountability

16 Ce principe directeur consacré par le considérant 74 du Règlement, dicte le comportement que le responsable du traitement doit adopter dans le cadre du traitement des données, à dessein de protéger les données à caractère personnel tout au long de la collecte. L'étude de la signification du principe (**paragraphe 1**), permettra de mieux comprendre les implications engendrées par l'accountability (**paragraphe 2**).

§1 - La consécration d'un principe de responsabilisation

17 La présence du principe d'accountability dans le règlement est nouvelle. Cela étant, l'astreinte des entreprises au respect de l'accountability n'est pas récente et se retrouve dans des domaines plus larges que la protection des données à caractère personnel. Principe directeur d'origine anglo-saxonne (**A**), l'accountability a été considérée en Europe comme une nécessité dans la protection des données (**B**).

[17]Le principe est évoqué à titre liminaire en considérant n°74, mais à la lecture du Règlement, il est certain que l'accountability dicte le comportement que doit adopter le responsable du traitement.

A. **Un principe d'origine anglo-saxonne**

18 Avant d'être utilisé dans le contexte de la protection des données à caractère personnel, le terme « accountability » se référait à l'obligation des mandataires de rendre compte à leurs mandants. Ainsi, l'accountability peut s'illustrer dans le cas des élus, des institutions publiques, qui doivent rendre compte à leurs électeurs : le gouvernement doit rendre compte au Parlement et aux citoyens. De même, l'accountability s'applique dans le cadre du droit des sociétés : les mandataires sociaux doivent rendre compte aux actionnaires de la société[18].

19 Le principe d'accountability est d'origine américaine et fait l'objet de réglementations dans nombre de matières juridiques. La pratique montre qu'outre l'aspect de mise en conformité de l'entreprise avec la réglementation applicable[19], un autre aspect important du principe est la délégation par l'autorité régulatrice de certains pouvoirs normatifs. Cette délégation s'accompagne du devoir de rendre compte de la bonne exécution de sa mission. Ainsi l'entreprise doit disposer d'une structure de gouvernance pour assurer la qualité de la norme qu'elle crée.

20 Lorsque l'on parle d'accountability dans le cadre des données personnelles, l'idée est renvoyée aux systèmes de gouvernance de la conformité mis en place au sein de groupes multinationaux et à l'obligation de démontrer la conformité au régulateur en cas de contrôle. En dehors du cadre purement américain, le concept n'est pas nouveau dans le domaine de la protection des données personnelles. Dès 1980 on le retrouve dans les lignes directrices[20] de l'OCDE avec un paragraphe intitulé « *Accountability principle* ». L'OCDE affirmait déjà la responsabilisation du maitre de fichier quant au respect des mesures donnant effet aux principes des Lignes directrices. Une norme ISO[21] de 2011 relative à la vie privée inclut également une section intitulée « *Accountability* ». Selon l'ISO, l'accountability est une obligation de diligence[22] à laquelle s'ajoute l'adoption de mesures concrètes et pratiques assurant la protection des données.

---

[18]Sur ces illustrations, v. W. Maxwell, « l'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles », *Dalloz IP/IT* 2016 p. 123

[19] Une mise en conformité au sens large : lois sur l'environnement, la comptabilité, la concurrence, etc.

[20] art. 14 Principe de responsabilité, *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfontalières de données à caractère personnel, OCDE*, 1980, révisées en 2013

[21] L'Organisation Internationale de normalisation (ISO) établit les documents qui définissent des exigences, spécifications, lignes directrices à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services (Normes internationales).

[22] Traduction de « *Duty of care* »

21 En définitive, le principe d'accountability signifie bien une obligation du responsable du traitement à la mise en conformité de ses traitements de fichiers, ce qui implique l'adoption de mesures concrètes afin d'assurer la protection des données à caractère personnel. Cette obligation qualifiée de diligence, passe par une délégation de certains pouvoir normatifs, ayant pour conséquence en cas de contrôle, la nécessaire démonstration du respect de ses obligations par le responsable du traitement.

B. **L'expansion du principe dans l'Union européenne**

22 Au niveau européen, la directive de 1995 ne fait pas spécifiquement référence à la notion d'accountability, mais certaines dispositions de la directive induisent implicitement le respect du principe. Notamment, on retrouve l'obligation du responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données[23]. Cependant cette obligation est cantonnée à la seule sécurité du traitement, afin d'empêcher notamment tout traitement non autorisé des données[24].

23 La consécration du principe d'accountability dans le Règlement tient compte de l'avis[25] rendu par le Groupe de travail de l'article 29[26]. Dans cet avis, l'article 29 avait conseillé la Commission européenne sur la manière de modifier la directive 95/46, aujourd'hui remplacée par le Règlement, pour favoriser la protection effective des données. L'article 29 avait suggéré d'établir un « *principe de responsabilité exigeant des responsables du traitement des données qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent* ». En 2010 déjà, en raison de la disparité des législations du fait de la transposition de la Directive 95/96/CE, la volonté d'imposer des responsables de traitements une démarche active afin d'assurer une protection effective et une conduite loyale dans le traitement des données se faisait déjà ressentir. A cette disparité des législations s'ajoute également le développement de nouvelles technologies pouvant être considérées comme dangereuses pour la protection des données personnelles, et n'ayant pas été prises en compte en

[23]Directive 95/46/CE, art. 17
[24]V. également le considérant 47 de la Directive 95/46/CE
[25]Avis n°3/2010 sur le principe de responsabilité, adopté le 13-7-2010 (G29 WP 173)
[26]Groupe de travail institué en 1996 par l'article 29 de la directive 95/46/CE, dit Groupe « Article 29 » ou « G29 », il s'agit d'un organe indépendant sur la protection des données et la vie privée

1995.

24 L'accountability est une notion difficilement traduisible dans toute sa signification en français. L'accountability ne saurait se restreindre à la simple responsabilité du responsable du traitement. L'accountability est à la fois l'affirmation en effet de la responsabilité de l'entreprise, mais il est surtout l'affirmation de la nécessité pour le responsable du traitement de démontrer qu'il a bien respecté les exigences règlementaires en matière de protection des données[27]. En cela, les choses seront différentes de ce qu'elles étaient sous l'empire de la Directive de 1995.

§2 - Un changement de perspective eu égard à la réglementation actuelle

25 L'entrée en application du règlement et ainsi du principe d'accountability marque la fin des formalités préalables exigées par la législation actuelle (**A**). Là n'est pas le seul changement opéré par l'adoption du principe d'accountability : l'exigence d'une responsabilisation de l'entreprise impose l'adoption de mesures responsabilisantes (**B**).

A. La fin des formalités préalables

26 Ce principe d'accountability sera nouveau en droit français, et renverse le système alors en vigueur : ce ne sera plus à l'autorité nationale de protection des données de mettre en exergue les manquements de l'entreprise[28]. Jusqu'alors en effet, la réglementation impose aux responsables du traitement des contraintes à priori, par la nécessité de déclarer les traitements auprès de l'autorité nationale compétence[29]. Avec l'entrée en application du règlement et du principe d'accountability, il y aura ainsi un renforcement de la responsabilité à postériori de l'entreprise, de par l'absence de déclaration du traitement à l'autorité compétente. Ce changement de perspective est aussi la conséquence de la délégation de certains pouvoirs normatifs à l'entreprise par l'autorité de régulation. Ce faisant, le règlement européen met fin

[27]Pour une telle information, v. E Jouffin, X. Lemarteleur et M-N. Gibon, « Le règlement sur la protection des données : les 10 commandements à connaître pour passer de la théorie à la pratique », *RDBF* n°4, Juillet 2016, étude 18
[28] V. point n°21.
[29] L. 6 janvier 1978, art. 22 et suivants

aux « formalités préalables » instaurées par la Directive de 1995[30].

27 Le règlement allège donc tout ce qui est contrôle a priori mais substitue une logique de conformité, dont les acteurs – responsables de traitements et sous-traitants, sont responsables[31]. L'obligation d'assurer la transparence et la traçabilité des opérations de traitement permettront à l'entreprise de rendre des comptes. En contrepartie de cet allégement des formalités cependant, il est prévu un contrôle plus strict du respect des obligations du responsable du traitement par les autorités de contrôle. Ce contrôle - et les sanctions pouvant être prononcées à l'encontre de l'entreprise-, seront de nature à assurer une mise en conformité effective, à tout moment du processus de traitement[32].

28 A présent, l'entreprise devra être en mesure de prouver que les traitements de données qu'elle met en œuvre respectent les règles applicables. En effet, le responsable du traitement doit démontrer activement la conformité de ses traitements à la règlementation, sans attendre que des irrégularités lui soient signalées par l'autorité de contrôle. Cette approche, mettant à la charge du responsable du traitement une démarche active dans la mise en conformité à la réglementation, n'a pourtant pas eu les faveurs du Conseil lors de l'adoption du texte. Notamment certaines délégations ont pu soutenir que les obligations prévues par le texte feraient peser sur les responsables de traitements une charge démesurée[33]. Aussi, le respect de l'accountability implique l'adoption de règles internes et la mise en œuvre des mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données est effectué dans le respect du Règlement.

[30] L'e-commerçant bénéficie d'une déclaration simplifiée, dans sa relation avec ses clients et prospects, conformément à l'article 24 de la Loi Informatique et Liberté. Il s'agit de la norme simplifiée n°48

[31]L. Costes, « La Cnil facilitatrice de l'évolution numérique », *RLDN*, N°136, 1er avril 2017

[32]E. Gabrié, « Les pouvoirs des autorités de protection des données », *Dalloz IP / IT* 2017 p. 268

[33]J.-S. Lefebvre, *Déjà 20 mois de négociations sur les données personnelles,* Contexte Numérique, 9 sept. 2015 Disponible sur : < https://www.contexte.com/article/numerique/donnees-personnelles-lobbying-americain-massif-a-bruxelles_20211.html >

B. **L'adoption de règles internes contraignantes**

29 L'article 24 du Règlement dispose que « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* »[34]. Le principe énoncé, encore convient-il de s'intéresser à la substance de cette obligation : comment se décline cette mise en conformité ?

30 L'article poursuit et décrit ainsi les obligations incombant au responsable du traitement pour se conformer au règlement. Au titre des mesures pouvant être adoptées pour assurer le respect de l'accountability, l'article 40 du Règlement encourage l'adoption par l'entreprise d'un code de conduite. Les codes de conduite constitueraient des « *instruments de promotion de la conformité permettant aux professionnels d'un secteur de rédiger des règles détaillées régissant leurs activités de traitement classiques et codifiant les bonnes pratiques* »[35].
Dans le domaine intéressant l'e-commerce, la Fédération européenne de Marketing Direct (FEDMA) a élaboré un code de politique européenne concernant l'utilisation des données à caractère personnel dans le domaine du marketing direct. Ce code a été soumis au groupe de l'article 29 qui l'a jugé conforme à l'article 27 de la directive 95/46/CE[36].

31 Le code de conduite est le texte élaboré par les associations et autres organismes représentant des catégories de responsables de traitements ou de sous-traitants, sur une initiative volontaire, et destiné à contribuer à la bonne application du Règlement européen, en tant compte de leurs secteurs et besoins spécifiques. L'article 40 du Règlement précise le contenu de ce code de conduite. La finalité de ce document est de préciser les modalités d'application du Règlement, « telles que :

- le traitement loyal et transparent ;
- les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ; (…) ;

[34]La différence avec l'article 17 de la Directive ne peut qu'être constatée : les mesures devant être adoptées ne se cantonnent pas à la sécurité du traitement.
[35]A. Bensoussan, *Règlement européen sur la protection des données – textes, commentaires et orientations pratiques*, Ed. Larcier, 2017, p. 256
[36]Avis 4/2010 du 13 juillet 2010 sur le code de conduite européen de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct (G29, WP 174).

- les mesures et les procédures visées aux articles 24[37] et 25[38], et les mesures assurant la sécurité du traitement visées à l'article 32[39] (…) ».

32 L'adoption de ces règles est nécessaire puisqu'avec la consécration de l'accountability, il revient au responsable du traitement de rapporter la preuve du respect de ses obligations. Il doit être à même de démontrer aux autorités de contrôle, ou à la personne concernée, sa politique de protection des données. En contrepartie de la simplification des formalités donc, le règlement prévoit l'obligation pour le responsable du traitement de conserver une trace documentaire de tous les traitements effectués sous sa responsabilité.

33 Le respect du principe d'accountability invite le responsable du traitement à revoir son organisation interne de traitement aux fins de mise en place d'une véritable gouvernance des données. L'accountability implique de nouvelles obligations en matière de sécurité et de protection des données à la charge du responsable du traitement. Notamment, le texte consacre le principe dit « *privacy by design* », et son corollaire- « *privacy by default* », obligeant le responsable du traitement à considérer la protection des données dès la conception de son projet et par défaut.

SECTION II - Le respect du principe de privacy by design and by default

34 Dans le cadre de la responsabilisation du responsable du traitement, celui-ci se voit assujetti à une nouvelle obligation de protéger la vie privée dès la conception et par défaut : privacy by design and by default. Après avoir consacré et énoncé le principe (**Paragraphe 1**) ; le Règlement envisage les moyens de mise en œuvre de celui-ci (**Paragraphe 2**).

[37] RGPD, art. 24 « Responsabilité du responsable du traitement »
[38]RGPD, art. 25 « Protection des données dès la conception et protection des données par défaut »
[39]RGPD, art. 32 « Sécurité du traitement »

§1 - La consécration du principe

35 Il convient d'aborder les origines du principe de protection des données dès la conception et par défaut (**A**), cela afin de mesurer les nouveautés engendrées pour le responsable du traitement français (**B**).

A. La genèse du principe

36 Le principe trouve son origine au Canada (***1***), et s'est ensuite développé en Europe (***2***).

1. Au Canada

37 Le concept de privacy by design and default a vu le jour au Canada dans les années 1990. Le commissaire à l'information et à la protection de la vie privée de l'Ontario alors en fonction est parti du constat que le cadre légal était insuffisant pour assurer une réelle protection de la vie privée. Il soulevait le fait qu'il fallait intervenir plus en amont du traitement. L'opérateur économique désirant traiter les données doit donc répondre à différentes exigences, notamment [40] :

- prendre des mesures procréatives et non réactives ; soit des mesures préventives et non correctives. Ainsi, l'opérateur économique doit s'interroger sur les incidences d'atteintes à la vie privée qui peuvent être consécutives à l'exploitation de la technologie envisagée ;
- assurer la protection implicite de la vie privée. A ce titre, l'opérateur économique doit s'assurer que l'utilisateur bénéficie d'une protection maximale, sans avoir aucune intervention à réaliser. Cela signifie que l'entreprise désirant traiter les données doit définir un niveau de protection maximale et s'assurer que la solution garantit ce niveau de protection, sans qu'aucun réglage par l'utilisateur ne soit nécessaire ;
- **intégrer la protection de la vie privée dans la conception des systèmes.** Aussi, il appartient à l'opérateur de prendre en compte la protection de la vie privée dès la

[40] A. Cavoukian, Information and Privacy Commissioner of Ontario, *Privacy by Design – The 7 foudational principles, Canada*, mai 2010

conception du système ;

- assurer la fonctionnalité intégrale selon « un paradigme à somme positive, et non à somme nulle ». Ce principe complexe de mise en œuvre suppose de concilier les intérêts des utilisateurs avec ceux de la société ;
- assurer la sécurité pendant toute la période de conservation des données ;
- assurer la visibilité et la transparence. Ce principe doit être assuré par une documentation réalisée par le responsable du traitement afin de de permettre notamment le droit d'accès de l'utilisateur ;
- respecter la vie privée des utilisateurs. Ce principe est une synthèse des autres principes évoqués précédemment. En effet, les exigences au titre du privacy by design ont pour objectif de respecter la vie privée des utilisateurs.

38 La mise en œuvre de ces principes est censée permettre la réduction des risques pour les utilisateurs des technologies, liés à un mauvais usage de leurs données. Cet objectif n'était pas assuré par le régime des formalités préalables[41]. Ce régime de protection en amont du projet doit permettre des comportements plus vertueux, là est l'objectif de ce nouveau mode d'autorégulation[42].

39 La prise en compte de ces principes et l'étude du modèle canadien permet de mieux appréhender le principe de privacy by design consacré par le règlement général sur la protection des données à caractère personnel.

2. En Europe

40 Le principe de protection des données dès la conception et par défaut figure notamment dans la communication de la Commission européenne « Une stratégie numérique pour l'Europe » et y est présenté de la manière suivante : « *le droit à la protection de la vie privée et des données personnelles est, dans l'Union européenne, un droit fondamental qu'il faut faire respecter effectivement (…) par tous les moyens possibles, depuis l'application généralisée du principe de « respect de la vie privée assuré dès la conception » dans les TIC concernées,*

[41]V. points n°26 et suivants

[42]M. Dary, « Privacy by Design : un principe de protection séduisant mais complexe à mettre en place », *Dalloz IP/IT* 2016 p. 476.

jusqu'aux sanctions dissuasives si nécessaire. ***Ce principe signifie que la protection de la vie privée et de données personnelles est prise en compte tout au long du cycle de vie des technologies, depuis le stade de leur conception jusqu'à leur déploiement, utilisation et élimination définitive*** **»[43].** Le Règlement introduit ce principe au sein de l'Union européenne, en cohérence avec la volonté du législateur de renforcer la protection des données à caractère personnel des personnes physiques.

B. **Une nouveauté en droit français**

41 Le droit national français ne connaît pas cette anticipation en amont du respect de la vie privée. Simplement l'article 34 de la Loi Informatique et Libertés énonce, pour l'heure, que le responsable du traitement est tenu de prendre « *toutes précautions utiles* » au regard de la nature des données et des risques présentés par le traitement ; mais seulement sous l'angle de la sécurité des données[44]. L'obligation consacrée par le règlement est plus large et gouverne tous les aspects du traitement ; sans être circonscrite à la seule sécurité des données[45]. Ainsi, alors que le responsable du traitement intervenait a posteriori, désormais celui-ci devra être proactif et agir en amont de chaque projet, en adoptant des mesures adéquates afin de protéger les données et la vie privée des individus. Force est de constater que le privacy by design constitue bien un prolongement du principe d'accountability.

42 L'article 25 du Règlement impose au responsable du traitement de mettre en œuvre, « *tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même* », des mesures techniques et organisationnelles appropriées. Ces mesures sont destinées à mettre en œuvre les principes relatifs à la protection des données « *de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* »[46]. Il s'agit donc pour le

[43]Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions, *Une stratégie pour l'Europe,* 19-5-2010, COM (2010) 245 final, pt 2.3. Confiance et sécurité.

[44]Voir précédemment pour le principe d'accountability, pris en compte par la Directive 95/46/CE seulement sous l'angle de la sécurité des données, point n°22

[45]Même si l'article spécifique à la sécurité du Règlement rappelle que le responsable du traitement est soumis au privacy by design quant à la sécurité des données : « *security by design* » ; ce qui atteste de l'importance du principe, qui gouverne toutes les phases du traitement.

[46]Voir également le considérant n°78 « […] *Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en*

responsable du traitement d'anticiper tous les risques liés au traitement de données via l'adoption de mesures « proactives » destinées à rendre l'individu maitre de ses données[47]. On pense notamment à des mesures assurant la confidentialité des données[48].

43 Le corollaire de cette protection des données dès la conception est la protection par défaut ; consacrée au paragraphe 2 de l'article 25. Le texte dispose ainsi que le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, « *par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées […] »*. Ce principe s'applique à la quantité de données à caractère personnel collectées, à l'étendue du traitement, ainsi qu'à la durée de conservation et à l'accessibilité des données.

44 Le principe de protection par défaut consacré par l'article 25 paragraphe 2 n'est pas sans rappeler le principe de minimisation des données. Ce principe de minimisation des données conduit à éviter de collecter et traiter des données à caractère personnel sauf si l'objectif recherché rend cette collecte indispensable. Si la collecte est indispensable, le principe de minimisation vient limiter le recours aux données à caractère personnel[49]. Le principe de minimisation des données apparaît dans le règlement « sous une peau de chagrin »[50], et l'on peut regretter à ce qu'il n'ait pas fait l'objet de plus de développements, afin d'astreindre au maximum les responsables de traitements à ne collecter qu'une partie infime des données fournies par les personnes concernées.

45 Si la consécration du principe de protection dès la conception et par défaut s'avérait nécessaire pour la protection des personnes physiques à l'égard des données à caractère personnel, la mise en œuvre du principe peut s'avérer plus complexe : la concrétisation pratique du principe n'équivaudra sans doute pas à sa consécration textuelle.

---

particulier, ***les principes de protection des données dès la conception et de protection des données par défaut […]* ».**

[47]Ce que prévoit expressément le considérant n°78 mentionné en note 46 : les mesures destinées à assurer la protection des données dès la conception et par défaut, pouvant consister « ***à permettre à la personne concernée de contrôler le traitement des données*** ».

[48] G. Haas, « Confidentialité et protection des données », *Dalloz IP/IT* 2017. 322

[49] Les procédés de minimisation étant les mêmes que ceux consacrés pour la protection de la vie privée par défaut : limite de l'étendue des catégories de données ; la quantité des données ; le caractère plus ou moins nécessaire de telles données ; ce qui atteste de ce que le principe de minimisation et de protection par défaut sont liés.

[50]A. Bensoussan, *Règlement européen sur la protection des données -- textes, commentaires et orientations pratiques*, Ed. Larcier, p. 15

§2 : La mise en œuvre du principe

46 L'article 25 du Règlement énonce, à titre d'exemples, des mesures techniques et organisationnelles permettant de s'assurer du respect du « privacy by Design » ; notamment la pseudonymisation des données (**A**). Force est de constater que l'abstraction de l'article engendrera une implémentation difficile du principe (**B**).

A. L'adoption de mesures techniques efficaces

47 Le respect du principe de protection des données dès la conception et par défaut suppose la mise en œuvre de mesures organisationnelles et techniques « appropriées ». Dans la phase de conception, comme dans les phases d'exploitation des données, les impératifs liés aux données à caractère personnel et aux traitements devront être pensés afin de permettre l'implémentation de ces mesures. Au titre de ces mesures, est encouragée la pseudonymisation, définie à l'article 4.3 b) du Règlement comme le traitement de données grâce auquel ces dernières ne peuvent être attribuées à la personne concernée sans utiliser une information supplémentaire, laquelle doit être gardée séparément et faire l'objet de mesures techniques et organisationnelles garantissant la non-attribution à une personne identifiée ou identifiable[51].

48 Le Règlement est clair. Premièrement, la donnée pseudonymisée est bien une donnée à caractère personnel, indirectement identifiante[52]. Ensuite, la pseudonymisation des données n'est pas une anonymisation et ne conduit pas à soustraire les données pseudonymisées de l'application du règlement[53]. Cette dernière affirmation, selon laquelle la pseudonymisation des données n'en réduit pas leur nature de données à caractère personnel, a été rendue nécessaire suite à la pression de certains lobbys, représentant en majorité les intérêts de responsable de traitements intervenant dans le domaine du marketing digital. Ces derniers souhaitaient évacuer du champ d'application du règlement les données pseudonymes, et ainsi s'affranchir du renforcement de leurs obligations ; considérant ne pas traiter de données personnelles en tant que telles, mais des données ayant subi des traitements ne permettant pas l'identification de la

[51] La pseudonymisation est également encouragée en tant que mesures afin de garantir la sécurité du traitement
[52] V. RGPD, consid. 26
[53] V. RGPD, consid. 28, allant à l'encontre des revendications de certains lobbys lors de l'adoption du projet de règlement européen

personne. On ne peut que saluer cette position de ne pas avoir consacré la notion d'anonymisation, et de ne pas avoir exclu du champ d'application du Règlement les données ayant subi un processus de pseudonymisation, surtout lorsque l'on sait en pratique que l'absence d'identification de la personne n'est pas absolue et irréversible[54]. Enfin, le Règlement favorise la pseudonymisation parce qu'elle est un moyen de réduire les risques pour les personnes et constitue un instrument d'équilibre entre intérêts contraires[55].

49 Plusieurs dispositions du règlement témoignent de la faveur du législateur européen pour la pseudonymisation et d'une incitation à la mettre en œuvre. La pseudonymisation est un moyen concret d'assurer le respect du principe de minimisation des données dès lors qu'elle est compatible avec la finalité du traitement[56]. C'est aussi une mesure concourant à la minimisation des données dès la conception et plus spécifiquement une mesure appropriée à mettre en œuvre par le responsable du traitement pour garantir un niveau de sécurité adapté au risque. Enfin c'est une mesure assurant la confidentialité des données et ainsi le respect de la vie privée de la personne concernée[57].

50 Ces mesures de pseudonymisation et de minimisation des données rentrent dans le cadre du devoir de penser à la protection des données dès la conception du projet et par défaut, et permettent ainsi d'assurer une plus grande protection des personnes physiques à l'égard de leurs données. Malgré la consécration textuelle de cette protection des données dès la conception et par défaut, l'implémentation de ce principe sera, en pratique, difficile à mettre en œuvre.

B. **La difficile implémentation du principe**

51 Beaucoup de questions se posent en pratique afin de mettre en œuvre le principe de privacy by design and by default. En effet, il faut s'interroger sur les technologies touchées par le principe, et les modalités concrètes de mise en œuvre des mesures objets de l'article 25 du Règlement. Aussi, la question de la mise en œuvre de cette nouvelle obligation aux traitements

[54] Des études universitaires montrent qu'à partir des données de recensement (seulement le code postal, le sexe et la date de naissance), il était possible de réidentifier 87% des citoyens nord-américains.
[55]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
[56]V. RGPD, art. 89
[57] V. note 48

en cours au jour de l'entrée en application du règlement est importante et épineuse. Les processus internes sont à revoir dès aujourd'hui, afin de s'assurer au lendemain du 25 mai 2018, que tout projet est par défaut protecteur des données personnelles des utilisateurs.

52 Nombreux sont ceux qui s'accordent sur le flou qui entoure les termes très généraux de ces principes. Prenons l'exemple du développement de l'air Big Data. Le terme « Big data » est apparu il y a une dizaine d'années pour désigner le traitement d'informations d'un volume gigantesque, dépassant les capacités de traitement alors utilisées[58]. Or, comment minimiser les données dans le but de respecter le principe de privacy by design alors que le big data trouve sa raison d'être dans le traitement de volumes gigantesques de données[59] ?

53 A la frontière d'obligations juridiques, informatiques, économiques et organisationnelles, la mise en œuvre pratique de la protection des données dès la conception et par défaut va nécessiter une coopération de l'ensemble des acteurs de l'entreprise et la mise en place d'une réelle stratégie de gouvernance des données. Elle contraindra les entreprises à élaborer en amont une véritable culture des données personnelles à l'ensemble des intervenants de l'entreprise[60].

54 Devant les contraintes imposées par cette nouvelle réglementation, il est légitime pour les opérateurs économiques de se poser la question de l'opportunité de mettre en œuvre ces dispositions. Le changement de paradigme qui passe désormais par une anticipation des risques constitue une opportunité de faire de la protection des données un élément de valorisation de leurs actifs. Cette valorisation peut notamment s'effectuer par le biais de la certification consacrée par le règlement[61]. Une entreprise qui respecte ses obligations et assure la protection de la vie privée dès la conception et par défaut pourra bénéficier d'un label qui sera un gage de confiance envers les personnes concernées[62]. En effet, le consommateur se rendant sur le site d'un e-commerçant labelisé sera plus à même de renseigner ses données à caractère personnel,

[58] Académie des technologies, *Big data : un changement de paradigme peut en cacher un autre,* 1e Ed., EDP Sciences, 2016, p.1

[59] I. Beyneix, « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *JCP G*, n°46-47, 9 novembre 2015, doctr. 1260

[60] Ce rôle devant sans aucun doute revenir au délégué à la protection des données

[61] RGPD, art. 42 : est encouragée « *la mise en place de mécanismes de certification en matière de protection des données ainsi que des labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement* ».

[62] A. Debet , « Les nouveaux instruments de conformité », *Dalloz IP/IT* 2016 p. 592

notamment des données bancaires nécessaires à une transaction commerciale à distance, que sur le site d'un e-commerçant n'ayant pas un tel label.

55 En se prémunissant et en anticipant les risques de l'utilisation des données personnelles, les entreprises vont regagner en confiance et se prémuniront notamment du vol de données ou autres failles de sécurité. L'application du principe d'accountability et de privacy by design est donc un moyen de préserver son activité commerciale et de conserver son image de marque. Le Règlement renforce aussi les obligations du responsable du traitement fondées sur le risque du traitement sur la vie privée de la personne concernée.

CHAPITRE II : L'ANALYSE DES RISQUES DU TRAITEMENT SUR LA VIE PRIVEE

56 De par l'astreinte du responsable du traitement à une démarche active dans la mise en conformité de ses activités de traitement, le règlement oblige le responsable du traitement à prendre en compte le risque engendré par le traitement sur la vie privée de la personne concernée, et plus généralement sur ses droits et libertés.

57 Outre l'obligation de procéder à une étude d'impact sur la vie privée lorsque le traitement présente des risques pour la vie privée de la personne concernée[63], qui peut aller jusqu'à une demande d'autorisation de l'opération à l'autorité de contrôle[64], l'approche par les risques du traitement encadre largement le recours par l'entreprise au profilage (**Section I**) et oblige le responsable du traitement à notifier les violations de données lorsqu'un risque existe pour les droits et libertés des personnes concernées (**Section II**).

SECTION I : L'encadrement du recours au profilage

58 Le développement des technologies permet l'analyse des historiques de navigation, des courriels et autres informations sur les réseaux sociaux et moteurs de recherche ; dans le but de connaître l'utilisateur en question. Le but de cette analyse est de permettre de proposer au consommateur des produits correspondants à ses besoins. Les abus constatés dans la pratique nécessitaient d'encadrer le recours au profilage et de donner la possibilité à l'utilisateur de reprendre le contrôle sur ses données utilisées à des fins de ciblage.

59 Prenant acte de l'ancrage de l'analyse prédictive et de la publicité ciblée comme technique classique en e-commerce (**paragraphe 1**), le Règlement conditionne le recours au profilage par le responsable du traitement (**paragraphe 2**).

[63]RGPD, art. 35 « Analyse d'impact relative à la protection des données »
[64]RGPD, art. 36 « Consultation préalable »

§1 : Une pratique classique d'e-commerce

60 Le recours au profilage est une évidence en commerce électronique, en tant que technique de marketing ciblé, tant il permet au commerçant d'augmenter ses ventes de par la proposition de contenus personnalisés au consommateur (**A**). Force est de constater les risques engendrés par la mesure de profilage (**B**).

A. La proposition de contenu personnalisé

61 Afin de voir à quoi consiste le profilage, il convient de le définir (***1***) et aussi d'envisager les technologies permettant de recourir au profilage (***2***).

1/ La définition du profilage

62 Le profilage permet de tracer les internautes dans le temps et sur différents sites, de créer des profils très précis, notamment de leurs goûts, de leurs caractéristiques, comme l'âge et le sexe, et d'afficher en ligne les publicités qui reflètent leurs intérêts. Au travers du big data, permettant l'accès à une quantité considérable de données, les entreprises pratiquent en effet une nouvelle sorte de marketing[65]. Ce marketing n'est plus fondé sur la segmentation de la clientèle, mais sur une caractérisation comportementale[66] permettant d'affiner, puis de personnaliser les offres de produits aux consommateurs.

63 La qualification de données « comportementales », objet du profilage, a un temps été un argument des spécialistes en marketing considérant que de telles données sont anonymes, et ne relèvent donc pas de la règlementation sur les données personnelles[67]. La CNIL refuse la soustraction de ces données du champ d'application de la Loi informatique et libertés, en ce que l'accumulation de données sur une seule et même personne et leur combinaison permettrait de

[65] E. Jouffin et X. Lemarteleur, « Du psautier de Mayence au zetaoctets – quel environnement juridique pour le big data ? » *: Banque et droit* 2016, n° 166, p. 12.
[66] G. Haas, *Guide juridique de l'e-commerce et de l'e-marketing*, Ed. ENI, coll. Data pro, 2015
[67] Sur les pressions exercées par les lobbys quant à la négation de qualification de données à caractère personnel, v. point n°48

la « *singulariser à partir d'un ou de plusieurs éléments qui lui sont propres* »[68], de sorte à ce que ces données doivent être considérées identifiantes et non anonymes.

64 Le profilage doit être appréhendé comme un processus s'appliquant à différentes techniques dont la première étape est la captation d'information et la deuxième étape, l'analyse de ces informations[69]. Il suffit de prendre l'exemple du client effectuant ses courses en ligne sur un site d'alimentation. L'e-commerçant va capter la commande de son client, et pourra l'analyser, de sorte à conclure que le client est un consommateur de produits exclusivement issus de l'agriculture biologique. La captation de ces informations et leur analyse permettra à l'e-commerçant de cibler ce client, en ne lui proposant à l'avenir, par exemple, que les promotions en lien avec son type d'alimentation.

65 Confortant cette vision du profilage, le Règlement définit le profilage en son article 4 §4 comme « *toute forme de traitement automatisé de données consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour* ***analyser ou prédire*** *des éléments concernant le rendement au travail, la situation économique, la santé, l****es préférences personnelles****, **les intérêts**, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».* Force est de constater l'étendue de la définition qui vise l'évaluation des « aspects personnels » de la personne concernée de manière large. Les acteurs du secteur du marketing attendent les lignes directrices du groupe de l'article 29, permettant l'interprétation de cet article.

66 Cette technique est très utilisée en pratique et permet tant bien à l'e-commerçant de proposer du contenu en adéquation avec le consommateur concerné ; qu'au consommateur de se voir proposer des produits et services en lien avec ses goûts.

[68] Délibération CNIL n°2013-420 du 3 janvier 2014

[69] Pour une telle analyse : J.Eynard, « les données personnelles, quelle définition pour un régime de protection efficace ? » : Ed. Michalon, 2013, p. 110

2/ Les techniques de profilage

67 La captation des données est rendue possible par la pose de cookies traceurs sur le terminal de l'utilisateur. L'analyse des données quant à elle est réalisée généralement par des algorithmes[70].

68 Les cookies sont de petits fichiers stockés dans la mémoire des ordinateurs, soit des informations déposées ou lues sur le terminal de l'utilisateur par les responsables d'application, lors de la consultation d'un site internet par exemple, et peu important le terminal utilisé par l'utilisateur (ordinateur, smartphone)[71]. Les cookies permettent de conserver une trace des actions de l'utilisateur du terminal et sont un outil de prédilection du profilage. Les algorithmes permettent l'analyse des données issues des cookies[72].

69 Conçu pour être au service du consommateur, en bénéficiant de services personnalisés et en évitant un démarchage répétitif et non-adapté aux centres d'intérêt, le profilage emporte cependant de nombreuses dérives.

B. **Les risques engendrés par la pratique**

70 Ce marketing prédictif est critiqué, tout d'abord par le consommateur, de par son caractère intrusif et surtout de par un sentiment de perte de contrôle dans la maitrise de sa navigation sur internet. Le risque du profilage est d'enfermer les individus dans un « déterministe numérique »[73]. En effet, la pratique représente un danger dans la mesure où elle influence les choix du consommateurs[74].

[70]Sur une analyse poussée du fonctionnement des algorithmes dans le commerce électronique : L. D. Godefroy, « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *D.* 2016 p. 438

[71] Pour cette proposition de définition : F. Mattatia, *Traitement des données personnelles : le guide juridique,* 2e Ed. Eyrolles, 2016 p. 44

[72]Commission Nationale de l'Informatique et des Libertés, *Ethique et numérique : les algorithmes en débat,* [en ligne] 23 janv. 2017
Disponible sur : <https://www.cnil.fr/fr/ethique-et-numerique-les-algorithmes-en-debat>

[73]*CE, rapport annuel 2014, p. 237 et s.*

[74]Allant jusqu'à réduire l'exercice de la liberté d'expression dans certains cas : E. Scaramozzino, « Le profilage encadré pour favoriser la diversité culturelle », *Juris art etc.* 2016, n°36, p.6

71 De plus, le propos a déjà été avancé, mais ces données censées être non identifiantes, peuvent, combiner entre elles, aboutir à des profils très précis de l'individu objet de la mesure. Surtout, le traitement de données à la base non identifiantes peut dégénérer en un traitement de données sensibles[75] ; cela sans avoir à respecter les règles contraignantes du traitement de données dites sensibles.

72 Le Règlement en son considérant 24 propose la soumission des traitements de données aux règles qu'il édicte lorsque le traitement est lié à l'observation du comportement des personnes concernées. Le texte continue et précise qu'afin de « *déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou analyser ou prévoir ses préférences, son comportement et sa disposition d'esprit* ». Ce suivi de la personne physique lors de sa navigation sur internet nécessite un contrôle du profilage, ce que le Règlement a opéré, obligeant le responsable du traitement à certaines contraintes dans la mise en œuvre du profilage.

§2 - Une pratique au recours conditionné

73 La consistance de la pratique ainsi que les risques et dangers engendrés nécessitaient un encadrement à l'échelle européenne du profilage. Aussi, le Règlement exige un traitement licite (**A**) ; ainsi qu'une communication à la personne concernée, qui est en droit de s'y opposer (**B**).

A. La licéité du traitement aux fins de profilage

74 Tout traitement de données à caractère personnel doit répondre à certaines conditions, dont notamment la licéité du traitement. Cela vaut surtout pour le profilage. Ainsi, le traitement doit reposer sur une base juridique. Dans le cas du traitement aux fins de profilage, il faut s'interroger sur la base juridique que constitue l'intérêt légitime du responsable du traitement

[75]Prenant l'exemple de l'e-commerçant spécialisé dans la vente agroalimentaire qui, en analysant les achats d'un client qui n'achète que des aliments hallal en vient à des données sur la confession religieuse.

(***1***). La licéité du traitement impose également au responsable du traitement de déterminer les finalités du traitement (***2***).

1/ L'intérêt légitime du responsable du traitement

75 L'article 6 du Règlement prévoit qu'un traitement n'est licite que dans la mesure où il satisfait l'une des conditions qu'il énumère. Il faut en effet que le traitement repose sur une base juridique, permettant sa mise en œuvre. Au titre des fondements du traitement, l'article 6 prévoit :

- le consentement de la personne concernée
- l'exécution d'un contrat entre le responsable du traitement et la personne concernée
- le respect d'une obligation légale du responsable du traitement
- la sauvegarde des intérêts vitaux de la personne concernée
- l'exécution d'une mission d'intérêt public
- les intérêts légitimes poursuivis par le responsable du traitement

76 Dans le cadre du profilage aux fins de prospection commerciale, le considérant 47 du Règlement énonce que le traitement de données à des fins de prospection peut être considéré comme répondant à un intérêt légitime du responsable du traitement. Certains auteurs critiquent le recours à ce fondement juridique comme base licite du traitement[76]. Une partie des commentateurs du texte européen estiment qu'à travers ce fondement, risque d'être autorisé tout traitement effectué par une société ayant une activité économique et commerciale, en ce qu'il serait légitime pour l'e-commerçant de rechercher un intérêt économique dans les traitements de données à caractère personnel de ses utilisateurs[77].

77 Cependant, l'absence de tournure affirmative du considérant 47 invite le responsable du traitement à manier avec prudence la base juridique de l'intérêt légitime. Notamment, le considérant 47 invite à ne pas utiliser ce fondement « *lorsque les intérêts ou les libertés et droits fondamentaux de la personne concernée (...) prévalent, compte tenu des attentes raisonnables*

[76]Sur l'ambiguïté de la notion et son recours : N. Metallinos, « 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
[77] Sur cette opinion : N. Martial-Braz, « Quel avenir pour la protection des données à caractère personnel en Europe ? *» : D.* 2013, p. 2788

des personnes concernées fondées sur leur relation avec le responsable du traitement ». Cette limite à l'intérêt légitime, fondée sur les risques du traitement dus au caractère intrusif du profilage, invite le responsable du traitement à faire reposer le traitement sur d'autres fondements, notamment l'exécution du contrat ou le consentement. Cependant, l'exécution du contrat ne constituera pas un fondement valable, en ce que la collecte à des fins publicitaires concernent des prestations accessoires au contrat. Le consentement sera alors exigé.

2/ La détermination des finalités du profilage

78 L'article 5-b du Règlement rappelle que les données doivent être traitées en vue de « *finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités* ». L'article 5-c ajoute que ces données doivent en outre être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées[78].

B. **L'information du consommateur**

79 Le règlement prévoit une obligation d'information et une obligation de permettre une opposition spécifique au bénéfice de la personne concernée par le profilage (***1***). De manière extrapolée, il convient d'évoquer la réforme de la directive « vie privée et communications électroniques »[79] qui viendra directement impacter le recours au profilage (***2***).

1/ L'obligation d'information sur la logique du profilage

80 Le responsable devra fournir à la personne concernée une information sur le profilage, la logique sous-jacente de la pratique ainsi que les conséquences prévisibles de ce traitement pour la personne concernée. Outre cette obligation d'information au bénéfice de la personne concernée ; le responsable sera obligé de prévoir un droit d'opposition au profilage.

[78]Application du principe de minimisation des données
[79]Directive 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (CE/2002/58)

81 Au titre du droit d'opposition général, l'article 21-1 du Règlement énonce que la personne concernée a le droit de s'opposer à tout moment à un traitement des données la concernant – traitement fondé sur l'intérêt légitime du responsable du traitement. Ainsi la personne concernée peut se prévaloir d'un droit d'opposition au profilage dans la mesure où celui-ci est lié à de la prospection commerciale. L'information de ce droit d'opposition devant être « *explicitement porté à l'attention de la personne concernée* » et *« présenté clairement et séparément de toute autre information* »[80].

82 L'avancée opérée par le Règlement sera complétée par une révision de la directive 02/58/CE, venant parachever la protection des personnes concernées par un traitement à des fins commerciales. Une refonte de la réglementation relative aux cookies, outils de prédilection du profilage, est en marche, rendant la problématique du profilage encore plus complexe et floue.

2/ Vers un contrôle plus accru du profilage

83 L'autre pilier de la protection des données à caractère personnel des personnes physiques est la directive de 2002 sur la protection de la vie privée dans le secteur des communications électroniques[81]. Cette directive prévoit, entre autres, le système de l'opt-in pour la prospection commerciale notamment par courrier électronique, et comporte également des dispositions sur les cookies et autres formes d'accès ou d'inscription sur les équipements terminaux des utilisateurs. La Commission européenne a lancé le 11 avril 2016 une consultation publique sur l'évaluation et la révision de cette Directive. Depuis, la Commission européenne a publié le 10 janvier 2017 sa proposition de révision de la directive e-privacy. Il s'agit d'un projet de règlement européen[82], texte d'application directe et contraignant, qui propose de remplacer cette directive et de moderniser la réglementation relative aux cookies et autres traceurs. L'ambition principale de ce texte est la volonté de la Commission à ce qu'il entre en application en même temps que le Règlement, soit le 28 mai 2018.

[80]RGPD, art. 21§4
[81]Directive dite « e-privacy » ou encore « vie privée et communications électroniques »
[82]Proposition de règlement du Parlement européen et du Conseil relatif au respect de la vie privée et à la protection des données personnelles dans les communications électroniques et abrogeant la directive 2002/58/EC, n°COM (2017) 10 final, 2017/003 (COD)

84 Le but est d'harmoniser totalement la législation applicable aux données. Le projet de règlement vise à protéger la vie privée des utilisateurs de services de communication, quelle que soit la nature des données, personnelles ou non. La proposition prévoit de renforcer les règles actuelles sur les cookies et autres traceurs[83], mais également d'étendre le principe de l'opt-in à l'ensemble du marketing direct envoyé par voie électronique[84].

85 En changeant la réglementation relative aux cookies ; c'est directement la pratique du profilage qui est impactée en ce que celle-ci est rendue possible par le placement de cookie sur le terminal de l'utilisateur afin d'étudier sa navigation et établir son profil[85]. Les cookies publicitaires sont directement visés. Ces cookies publicitaires sont considérés comme des cookies tiers, à la différence des cookies posés par l'éditeur du site lui-même[86]. Dans ce nouveau cadre, le navigateur devient le socle de l'acceptation des cookies tiers. En effet, la proposition de règlement impose aux navigateurs de proposer un paramétrage dédié aux cookies tiers par l'individu. Ce dernier choisira de les accepter ou non une bonne fois pour toute.

86 Le secteur de la publicité s'inquiète de cette centralisation du paramétrage et de l'offre publicitaire au niveau du navigateur. Les éditeurs de site craignent également de ne plus pouvoir interagir directement avec leurs utilisateurs pour le recueil du consentement aux cookies tiers déposés via leur site[87]. De même le groupe de l'article 29 n'est pas satisfait de cette proposition, et souhaite que les navigateurs offrent une « granularité » à leurs utilisateurs pour accepter ou refuser les cookies selon leur finalité[88].

87 Force est de constater que les risques engendrés par la pratique du profilage, notamment sur la vie privée des personnes entrainent un mouvement européen tendant à renforcer les obligations des entreprises recourant à la pratique. Le Règlement prend acte de ce renforcement des obligations du e-commerçant en la matière. L'approche par les risques opérée par le règlement se manifeste également par un renforcement des obligations du responsable du traitement dans le cas d'une violation des données personnelles sous son contrôle.

---

[83] Art. 8§1 de la proposition de règlement
[84] Art. 16 de la proposition de règlement
[85] V. point n°67 et suivants
[86] G. Haas, *Guide juridique de l'e-marketing*, Ed. ENI, sept. 2013
[87] V. notamment L. Boulet et L. Frossard, « Un an de droit de la publicité », *CCE* n°7-8, juillet 2017, chron. 9
[88] Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), adopted on 4 April 2017 (17/ZN/WP247)

Section II : La notification des violations de données

88 L'approche par les risques du traitement passe également par un renforcement de l'obligation de sécurité de l'entreprise. Outre l'encadrement de la sécurité du traitement prévu à l'article 32 du Règlement ; le texte prévoit de nouvelles dispositions consacrées à la violation de données. Ces nouvelles dispositions prennent surement acte des incidents constatés en la matière et de leurs conséquences pour les personnes concernées.

89 Force est de constater que le règlement renforce de manière significative la sanction en cas de non-respect des obligations en matière de violation de données. A l'heure actuelle, la violation de l'obligation de notification d'une violation de données à caractère personnel auprès de la CNIL, est puni 150 000 euros lors du premier manquement, et de 300 000 euros d'amende en cas de réitération du manquement[89]. Outre le fait que la sanction ne concerne que les fournisseurs de services de communications électroniques accessibles au public ; avec l'entrée en application du Règlement, les violations de sécurité pourront donnent lieu à une amende dont le montant maximal est de 10 millions d'euros, dans le cas d'une entreprise « jusqu'à 2% du chiffres d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »[90].

90 Afin d'éviter la condamnation à une telle amende administrative, le responsable du traitement devra respecter son obligation de notification des violations de données en cas de risque pour les personnes concernées, l'astreignant à coopérer avec l'autorité de contrôle (**Paragraphe 1**) ; ainsi qu'à communiquer avec la personne concernée par la violation des données (**Paragraphe 2**).

§1 : Une coopération avec l'autorité de contrôle

91 La notification à l'autorité de contrôle en cas de violation des données à caractère personnel envisagée par le texte prévoit une coopération efficace (**A**). La réalité de cette notification se révèlera, en pratique, plus difficile à mettre en œuvre (**B**).

[89] L. 6 janvier 1978, art. 47
[90] RGPD, art. 83§4 a)

A. Une coopération textuelle efficace

92 Le considérant 85 du Règlement relève qu'une « *violation de données à caractère personnel risque, si l'on n'intervient pas à temps et de manière appropriée, de causer aux personnes physiques concernées des dommages physiques, matériels, ou un préjudice moral tels qu'une perte de contrôle sur leurs données à caractère personnel ou une limitation de leur droits* ». Le considérant va plus loin en envisageant « *une discrimination, un vol ou une usurpation d'identité* » comme conséquence de la violation des données.

93 La pratique montre la réalité des risques énoncés par le considérant. Cette réalité peut être illustrée par le hackage dont ont été victimes les utilisateurs du site YAHOO. En effet en septembre 2016, YAHOO a affirmé avoir été victime d'un piratage dans lequel plus de 500 millions de comptes utilisateurs avaient été affectés. De nombreuses données personnelles ont ainsi été dérobées, notamment les dates de naissance, noms, adresses électroniques et mots de passe[91]. Un autre cas mérite d'être soulevé : en mai 2016, les données de plus de 117 millions d'utilisateurs du site professionnel LinkedIn avaient été mises en vente sur un site spécialisé dans ce type de recel[92]. Cette pratique est courante et consiste à revendre les données des utilisateurs et à les transmettre à d'autres opérateurs afin que ceux-ci puissent, notamment, procéder à de la prospection commerciale envers les personnes dont les données ont été recueillies. Un encadrement à l'échelle européenne était nécessaire ; visant à renforcer les obligations du responsable du traitement dont le système de traitement automatisé fait l'objet d'une violation de données.

94 L'article 33 du Règlement vient encadrer la notification à l'autorité de contrôle compétente en cas de faille de sécurité. Cet article est inspiré de la notification des violations de données à caractère personnel prévue à l'article 4, paragraphe 3, de la directive 2002/58/CE « Vie privée et communications électroniques » [93]. En cas de violation de données à caractère

[91]Le Monde, *500 millions de comptes, d'utilisateurs Yahoo ! ont été piratés*, [en ligne] Chronique des (r)évolutions numériques, 22 sept. 2016
Disponible sur : <http://www.lemonde.fr/pixels/article/2016/09/22/500-millions-de-comptes-d-utilisateurs-de-yahoo-ont-ete-pirates_5002118_4408996.html>

[92]Julie Lausson, *167 millions d'accès Linkedln piratés : le vôtre aussi ?*, [en ligne] Numerama, 24 mai 2016 Disponible sur : <Numerama,http://www.numerama.com/tech/172291-167-millions-dacces-linkedin-pirates-le-votre-aussi.html>

[93] Pour plus de détails sur le système alors en vigueur ; v. notamment : Eric A. Caprioli, « Données à caractère personnel et sécurité, notification des violations de données à caractère personnel », *CCE* n°2, décembre 2011, comm. 116

personnel, le responsable du traitement devra en notifier la violation en question à l'autorité de contrôle compétente, dans les meilleurs délais et si possible 72h au plus tard après en avoir pris connaissance. Le texte prévoit une exception à cette obligation, dans le cas où la violation en question n'est pas susceptible d'engendrer « *un risque pour les droits et libertés des personnes physiques* ». Le sous-traitant doit notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance. Cette célérité requise pour la notification au responsable du traitement n'est pas requise dans les cas où la violation « *n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* »[94].

95 La notification à l'autorité de contrôle doit s'accompagner des éléments de nature à instruire l'autorité ; notamment devront être communiquées, « *à tout le moins* »[95] :

- la description de la nature de la violation, les catégories et nombre de personnes concernées, ainsi que les catégories et nombre approximatif d'enregistrements de données concernées
- les coordonnées du délégué à la protection des données,
- les conséquences probables de la violation
- les mesures prises ou que le responsable du traitement propose de prendre, pour remédier à la violation de données ; ainsi que les mesures pour atténuer les éventuelles conséquences négatives.

Cette notification doit par ailleurs être documentée, ce qui permet à l'autorité de vérifier le respect des obligations du responsable du traitement instituées par l'article 33.

96 Si les dispositions de l'article sont claires quant au déroulement de la notification par le responsable du traitement à l'autorité de contrôle, il apparait à la lecture de l'article que la mise en œuvre de cette notification pourra s'avérer ardue.

[94]RGPD, art. 33§1
[95]RGPD, art. 33§3 ; l'emploi du terme « à tout le moins » ne conférant pas à cette liste de caractère exhaustif.

B. **Une coopération complexe en pratique**

97 Cette notification des violations de données et cette coopération requise avec l'autorité de contrôle paraît séduisante et garante de la protection des données des personnes physiques. En pratique, les exigences textuelles seront difficiles à mettre en œuvre pour plusieurs raisons. Il convient en effet de ne procéder à la notification qu'en cas de risque pour les droits et libertés des personnes physiques (**1**). Surtout, le responsable du traitement est astreint à un délai de notification qui peut s'avérer court (**2**).

1. La détermination d'un risque pour les droits et libertés des personnes physiques

98 Le texte permet de passer outre la notification de la violation de données si celle-ci « *n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* ». Cette évaluation devra être maniée avec prudence par le responsable du traitement victime d'une violation de données. Il conviendra d'évaluer précisément les données objets de la violation, afin de ne pas considérer de manière trop hâtive qu'une violation de données n'est pas susceptible d'engendrer un risque pour les personnes physiques[96]. Selon la Commission du marché intérieur et de la prospection des consommateurs, sollicitée pour avis sur le projet de règlement[97], l'obligation de notification des failles de sécurité ne s'imposerait pas lorsque les données ne peuvent être lues[98], dans la mesure où « la notification n'apporte aucune amélioration aux citoyens en matière de respect de la vie privée dans une telle situation ».

99 En pratique on peut supposer et anticiper le fait qu'un responsable du traitement, dont le système informatique fait l'objet d'une violation de données personnelles, procèdera à cette notification et s'engagera à collaborer avec l'autorité de contrôle, même si le risque de cette violation est minime. Cela, et cet argument est compréhensible, par peur de faire l'objet d'une amende administrative lourde de conséquences.

[96]Cette absence de notification pouvant être considérée comme fautive et les sanctions sont lourdes v. point n° 89
[97]Rapport sur la proposition de règlement, Jan Philipp Albrecht, Doc. A7-0402-2013 du 21-11-2013, Amendement 64, p. 477.
[98]Tel est le cas des données fortement chiffrées

100 D'ici le 26 mai 2018, on peut espérer des lignes directrices de la part du groupe de l'article 29 sur l'interprétation qu'il convient d'avoir sur le « *risque* » pour les droits et libertés des personnes physiques. Là ne s'arrête pas les difficultés pratiques engendrées par le texte.

2. Le délai de notification de 72 heures

101 Le délai dans lequel la notification doit être adressée à l'autorité de contrôle compétente a fait l'objet de débats et d'amendements. Dans la version initiale du Règlement, ce délai était de 24 heures[99]. La solution finalement retenue étant « dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance », en ce qui concerne le responsable du traitement, et « dans les meilleurs délais après en avoir pris connaissance », en ce qui concerne le sous-traitant. Le respect de cette diligence ne sera pas aisé pour le responsable du traitement pour plusieurs raisons[100].

102 Premièrement, on peut se demander si ce délai de 72 heures ne servirait pas justement à examiner si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, comme cela est exigé par l'article 33[101]. Aussi, ce délai de 72 heures n'est-il pas trop bref si l'on observe les exigences formelles requises pour la notification ?[102] A tout le moins, n'aurait-il pas été préférable de prévoir une obligation de notification de la violation de données dans les 72 heures, sans prévoir de forme particulière pour cette notification, et ensuite d'exiger la communication des éléments visés au paragraphe 3 de l'article 33 dans un délai raisonnable à compter de cette première notification ?

103 Enfin, en cas de recours à un sous-traitant, il faudra une véritable collaboration de celui-ci puisque le sous-traitant est également astreint à respecter cette obligation « dans les meilleurs délais » et à aider le responsable du traitement à documenter et remédier à cette violation. Ce délai étant court, le responsable du traitement devra définir les règles de remontée

[99]La Commission des libertés civiles, de la justice et des affaires intérieures a accepté la suggestion du rapporteur Jan Philipp Albrecht, de faire passer de 24 à 72 heures le délai de notification d'une violation de données à caractère personnel à l'autorité de contrôle ; V. note 97, Amendement 170, p. 526.

[100] V sur ce propos : A. Bensoussan, *Règlement européen sur la protection des données, textes, commentaires et orientations pratiques*, Ed Larcier, p. 221

[101] V. point n°98

[102] V. point n°95 et RGPD, art. 33§3

d'informations dans les contrats conclus avec les éventuels sous-traitants[103]. Cette collaboration entre responsable du traitement et son sous-traitant dans le cadre de la violation de données à caractère personnel n'est qu'une application particulière de la réorganisation des relations des parties prenantes au traitement[104]. Mais il convient de relativiser l'incertitude et la crainte laissée par le texte et la sanction de son manquement. En effet, alors que jusqu'à maintenant seul le responsable du traitement était responsable de tout manquement à la règlementation sur les données personnelles, et notamment des failles de sécurité ; aujourd'hui les responsabilités sont clairement établies et le sous-traitant peut voir sa responsabilité engagée[105].

104 Force est de constater le flou laissé par la lettre de l'article 33 et les incertitudes qui planeront à compter du 26 mai 2018. A l'instar de notre droit des contrats français, faisant souvent référence à la notion « dans les meilleurs délais », il convient d'espérer que la notion sera appréciée au cas par cas, selon chaque violation de données constatée. Mais l'intérêt de la souplesse de la notion de notification dans les meilleurs délais perd de son intérêt lorsqu'elle est elle-même renfermée dans un délai de 72h.

§2 : Une communication à la personne concernée

105 Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à la personne concernée dans les meilleurs délais[106]. Cette notification devant s'opérer « *en des termes clairs et simples* » et décrivant la nature de la violation de données à caractère personnel ainsi que les informations visées dans la notification faite à l'autorité de contrôle. Le paragraphe 4 de l'article 34 énonce que l'autorité de contrôle pourra, après avoir examiné si cette violation est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication, si celui-ci n'y a pas procédé.

[103]Notamment par le biais d'une annexe dite PAS (Plan d'Assurance Sécurité) ; annexe dédiée aux données

[104] A. Banck, « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT* 2017 p. 36

[105] RGPD, art. 82 § 1 : « *Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'**obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi** ».*

[106] RGPD, art.34

106 Le texte n'oblige le responsable du traitement à informer à la personne concernée que si la violation entraine un « risque élevé pour les droits et libertés de la personne concernée ». La notion de « risque élevé pour les droits et libertés de la personne concernée » engendre des interrogations sur l'interprétation à opérer. En effet, si le règlement tend à accroitre considérablement la protection des personnes physiques à l'égard de leurs données à caractère personnel, ne devrait-on pas considérer que toute violation de données constitue « un risque élevé pour les droits et libertés de la personne » ? Le responsable du traitement devra donc apprécier si la communication à la personne concernée par la violation de données est nécessaire. Il convient d'observer que le « risque » envisagé pour la communication à la personne concernée n'est pas le même que celui envisagé pour la notification à l'autorité de contrôle. En effet, l'article 33 exige une notification à l'autorité de contrôle si la violation de données est « susceptible d'engendrer un risque » pour les personnes physiques ; alors que l'article 34 n'exige une communication à la personne concernée que si cette violation est susceptible d'engendrer un « risque élevé » pour les droits et libertés de la personne concernée. Pour reprendre l'avis du rapporteur Jan Philipp Albrecht, la différenciation tient sans doute à éviter à la personne concernée une « lassitude éventuelle », qui ainsi ne sera avertie d'une violation qu'en cas de risque réel[107].

107 Outre l'absence de communication en cas d'absence de risques élevés pour les libertés et droits de la personne concernée, le Règlement européen dispense de communication la violation si :

- des mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre, notamment des mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, tel que le chiffrement
- le responsable du traitement a pris « des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser »
- la communication « exigerait des efforts disproportionnés »

[107] V. Note 97, Exposé des motifs, p. 225

108 La communication à la personne concernée s'inscrit dans les exigences de la nouvelle règlementation visant à garantir la transparence[108]. L'article 34 paragraphe 2 précise d'ailleurs que la communication doit décrire « en des termes clairs et simples » la nature de la violation de données. La transparence est un nouveau principe gouvernant le règlement et qui s'applique également à l'information de la personne concernée, comme il pourra être constaté ultérieurement.

109 Le renforcement des obligations du responsable du traitement, par la nécessité de mettre en place un système de gouvernance des données, et à prendre en compte le risque du traitement sur la vie privée des personnes concernées, renforce de manière indirecte la protection conférée aux personnes physiques. En effet, elle ne concerne pas directement la personne, mais elle est un préalable nécessaire, un socle de confiance pour la personne concernée par le traitement. L'obligation de protéger les données, de manière générale, devra être mise en avant par l'e-commerçant dans sa relation avec ses clients et prospects. La protection des données est devenue un défi pour les responsables de traitements et permettra de valoriser la marque du e-commerçant qui pourra ainsi continuer à effectuer des ventes indirectes.

110 De manière plus directe, le Règlement renforce la protection des consommateurs à l'égard de leurs données personnelles en renforçant leurs droits. Ce renforcement passe par la consolidation des droits existants ainsi qu'à la création de nouveaux droits.

[108] I. Gheorghe-Badescu, « Le nouveau règlement général sur la protection des données, quoi de neuf ? » *R. UE* 2016 p. 466

PARTIE II : LE RENFORCEMENT DES DROITS DES CONSOMMATEURS

111 « *Le centre de gravité de la nouvelle législation demeure la personne* »[109]. Le Règlement concrétise un renforcement de la protection des données personnelles et une plus grande maitrise des données par la personne physique concernée. Cette plus grande maitrise sera rendue possible par le renforcement des droits existants et la consécration de nouveaux.

112 Outre le renforcement des droits d'accès, de rectification[110] et d'effacement111, le Règlement renforce de manière significative le droit à l'information et le consentement donné par la personne physique au traitement de ces données, renforçant ainsi les droits préalables à la collecte des données (**Chapitre I**). Considérée comme l'une des grandes nouveautés du règlement, la consécration d'un droit à la portabilité viendrait parachever la protection des personnes concernées par un traitement à des fins commerciales (**Chapitre II**).

[109] Conférence de presse du 27 mars 2017, rapport d'activité 2016 et des enjeux 2017, CNIL
[110] Ces droits sont classiques dans le cadre du commerce électronique et ne subissent pas d'impact majeur avec la nouvelle réglementation européenne.
[111] Le droit d'effacement, autrement dénommé « droit à l'oubli » est une avancée significative dans le cadre du renforcement de la protection des données à caractère personnel, mais il ne concerne pas tant les acteurs du commerce électronique traditionnel, mais plutôt les réseaux sociaux.

CHAPITRE I : LE RENFORCEMENT DES DROITS PREALABLEMENT A LA COLLECTE

113 Avant d'envisager les avancées du règlement européen en la matière, il convient de rappeler les règles applicables en matière de prospection commerciale, montrant ainsi l'importance de l'information et du consentement de la personne concernée. En effet, la prospection commerciale est soumise à une information préalable et au recueil du consentement de la personne concernée par le traitement[112].

114 A l'heure actuelle, le responsable du traitement est soumis aux obligations prévues par l'article 32 de la loi informatique et liberté l'astreignant de fournir une information à la personne concernée, au moment de la collecte et non uniquement dans les conditions générales d'utilisation[113]. De plus, est requis le consentement de la personne concernée, préalablement à tout traitement portant sur ses données114. La pratique actuelle pour recueillir ce consentement consiste dans le système de « *l'opt-in* » matérialisé par une case à cocher par la personne concernée. L'opt-in suppose le refus par défaut de la personne concernée, mais demande un acte positif d'inscription pour marquer son consentement[115]. Ainsi, en cochant la case « *j'accepte de recevoir la newsletter de l'e-commerçant* », par exemple, la personne donne sa « manifestation de volonté libre, spécifique et informée »116 de recevoir de la prospection commerciale par email.

115 Le Règlement vient renforcer les droits de la personne concernée préalablement au traitement de ses données, contraignant le responsable du traitement à revoir ses processus de traitement avant l'entrée en application du règlement. Ce renforcement des droits préalablement au traitement des données, passe par la consécration d'une information transparence au bénéfice de la personne concernée (**Section I**). Mieux informée, la personne concernée sera à même de consentir valablement au traitement de ses données[117] (**Section II**).

---

[112] Pour une explication plus détaillée, V. Gérard Haas, *Guide juridique de l'e-commerce et de l'e-marketing*, Ed. ENI, coll. Data pro, 2015

[113] V. également l'interprétation faite de l'article 32 de la loi par la CNIL dans la délibération n°2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (NS-048)

[114]Pour la prospection commerciale par e-mail : art. L. 33-4-1 du Code des postes et télécommunications

[115] F. Mattatia, *Traitement des données personnelles : le guide juridique,* Ed. Eyrolles 2013, p. 25

[116] Ibid.

[117]Ou, lorsque le traitement n'est pas fondé sur le consentement ; la personne sera à même d'exercer les droits faisant l'objet de l'information, voir notamment pour le profilage point n°80 et suivants

SECTION I : Une information transparente

116 A titre liminaire de l'énoncé des droits de la personne concernée, le Règlement prévoit deux sections spécifiques relatives à l'information de la personne concernée : une information au titre du traitement de ses données et une information au titre de l'exercice de ses droits[118]. Le renforcement de l'information des personnes concernées est l'un des leviers mis en place par le règlement, pour accroitre la protection des personnes physiques dont les données sont traitées.

117 De nouveaux principes généraux applicables à la collecte et au traitement des données à caractère personnel viennent renforcer les principes traditionnels de loyauté et de licéité[119] du traitement. Un des principes consacrés par le règlement est le principe de transparence[120], partant du constat que les informations communiquées aux personnes concernées étaient souvent trop complexes et trop volumineuses. L'interprétation faite du principe de transparence dans le considérant 58 du Règlement se retrouve également dans le résumé de l'avis du contrôleur européenne de la protection des données[121], dans lequel il est précisé que « *les personnes concernées doivent recevoir des informations claires sur les données qui sont traitées, notamment les données observées ou déduites les concernant, être mieux informée sur la manière dont leurs données sont utilisées et sur les finalités pour lesquelles elles sont utilisées, y compris la logique algorithmique qui sert à déterminer les hypothèses et les prévisions à leur sujet* ».

118 Ce principe d'information transparente implique de fournir à la personne concernée une information complète (**paragraphe 1**) mais également de rendre cette information accessible (**paragraphe 2)**.

[118] RGPD, Section 1 « t*ransparence et modalités* » ; Section 2 « *Information et accès aux données à caractère personnel* »
[119] Pour le principe de licéité du traitement, appliqué au profilage, v. point n°74 et suivants
[120] Pour mesurer l'importance conférée au principe de transparence, voir notamment : RGPD, consid. 58, 60 et 61
[121] Avis n°7/2015 du Contrôleur européen à la protection des données (CEPD), *Relever les défis des données massives : un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes,* JO C 67, 20 fév. 2016. 13-15

§1 : L'exhaustivité de l'information

119 Le texte distingue le cas où les informations sont collectées directement (**A**) ou non (**B**) auprès de la personne concernée. Dans les deux cas, la longueur des articles, due au nombre d'informations à fournir, atteste bien de ce que le règlement exige une information complète et donc transparente.

A. L'information en cas de collecte auprès de la personne concernée

120 La collecte directe renvoie notamment à l'idée d'un renseignement des données par le biais d'un formulaire de souscription, par exemple lorsque le client se crée un compte de fidélité sur le site de l'e-commerçant. Les informations devant être communiquées par le responsable du traitement à la personne concernée dans ce cas sont énoncées à l'article 13 du Règlement. Il convient d'en mesurer l'importance en pratique. Ces informations sont :

- l'identité et les coordonnées du responsable du traitement et le cas échéant, du représentant du responsable du traitement
- le cas échéant les coordonnées du délégué à la protection des données
- **les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement**
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers s'ils constituent le fondement du traitement
- les destinataires ou les catégories de destinataires des données à caractère personnel
- le cas échéant, le fait que le responsable du traitement à l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers et les garanties encadrant ce transfert ainsi que les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition
- **la durée de conservation des données, ou lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée**
- l'existence du droit de demander au responsable du traitement l'accès aux données, la rectification ou l'effacement de celles-ci ou une limitation du traitement relatif à la personne concernée ou du droit de s'opposer au traitement et du droit à la portabilité des

données[122]

- lorsque le traitement est fondé sur le consentement, l'existence du droit de retirer celui-ci à tout moment[123]
- le droit d'introduire une réclamation auprès d'une autorité de contrôle
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère règlementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données ainsi que les conséquences éventuelles de la non-fourniture de ces données
- l'existence d'une prise de décision automatisée y compris le profilage et, au moins en pareils cas, les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée[124.]

121 Il n'y a pas de différence majeure avec ce qui est exigé pour l'heure par la loi Informatique et Libertés ; hormis l'ajustement prévu du fait de la création d'un délégué à la protection des données. La nouveauté par rapport aux informations communiquées sous la Loi Informatique et Libertés est l'ajout de l'information à la personne de (1) la durée de conservation des données au point 2.a) et (2) les finalités du traitement opéré et la base juridique du traitement au point 1.c). La communication de ces informations est un corollaire nécessaire à la consécration du principe de transparence et tend à rendre la maitrise aux personnes concernées par le traitement de leurs données.

122 Cette exigence d'informer la personne concernée par le traitement de ses données engendre tout de même certaines difficultés, notamment la nécessité pour le responsable du traitement de déterminer la durée de conservation des données, et surtout d'indiquer à la personne la finalité du traitement opéré, dans le cas où les données peuvent être utilisées pour plusieurs finalités.

[122] Plus de développement en Chapitre II « Un droit à la portabilité des données »
[123]Plus de développement à la section suivante : Section II « un consentement éclairé sur la base de l'information »
[124] V. Précédemment sur « L'encadrement du recours au profilage »

B. **L'information en cas de collecte auprès d'une tierce personne**

123 Les données peuvent être recueillies auprès d'une personne autre que la personne concernée, notamment, dans le cadre d'opérations de commerce électronique, en cas de cession de données ou via des opérations d'enrichissement des données par exemple[125]. Lorsque les données ne sont pas collectées directement auprès de la personne concernée, les mêmes informations sont à fournir en plus de celles prévues à l'article 14, soit :

- les catégories de données concernées
- la source d'où proviennent les données

124 Cette information doit intervenir dans un certain délai, qui sera, sans doute, difficile pour le responsable du traitement à respecter : « *dans un délai raisonnable après avoir obtenu les données, mais ne dépassant pas un mois* ». Dans le cadre du commerce électronique, la difficulté pour le responsable du traitement sera donc d'identifier la provenance des données, en raison du développement de l'air big data126. Cela influera certainement sur le respect du délai de communication à la personne concernée. L'identification de la personne ayant communiqué les données peut s'avérer complexe et ainsi la communication de la source d'où proviennent les données compromises.

125 L'exhaustivité de l'information n'est que le premier pendant de l'exigence d'une information transparente. La transparence de l'information exige également une information accessible.

§2 : L'accessibilité de l'information

126 L'accessibilité de l'information est le corollaire de l'exigence d'une information complète, partie intégrante du principe de transparence de l'information. La teneur du droit à une information accessible (**A**) rend compte des difficultés engendrées (**B**).

[125]Un exemple typique est l'enrichissement des adresses emails des clients de l'e-commerçant. L'e-commerçant, en tant que responsable du traitement, va confier à un prestataire, sous-traitant, la rectification des adresses emails figurant dans sa base de données client. Ainsi, une adresse inactive de l'e-commerçant mat.dupont@X.com sera enrichie par le prestataire qui travaillera et restituera la bonne adresse : mathieu.dupont@X.com.
[126]Sur ce point, v. note n°59

A. **La teneur du droit à une information accessible**

127 L'article 12-1 du Règlement impose que l'information communiquée soit « *concise, transparente, compréhensible et aisément accessible, {rédigée} en des termes clairs et simples* ». Dans ce contexte, l'accessibilité doit être entendue en tant que l'accès facile à l'information. Le 60e considérant du Règlement mentionne quant à lui que le principe de transparence exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités.

128 Le principe de transparence de l'information n'était pas expressément inclue dans la loi n°2004-801 du 6 aout 2004 transposant en droit national la Directive n°95/46/CE. L'article 32 II susmentionné prévoit simplement l'obligation pour le responsable du traitement d'informer « de manière claire et complète » la personne concernée par un traitement par des traceurs. Le projet de règlement envisageait l'instauration par le responsable du traitement d'une information normalisée sous forme d'icônes. Cette obligation a disparu dans le texte définitif, seule subsiste une recommandation d'adopter une illustration visuelle de l'information, notamment dans des cas où la multiplication des acteurs et la complexité des technologies engendrent une difficulté pour la personne concernée de savoir et comprendre si des données à caractère personnel la concernant sont collectées et pour quelle finalité[127]. Le Règlement cite expressément le cas de la publicité en ligne. Un acte délégué au Règlement viendra proposer une iconographie avant la date d'application du règlement.

129 Il appartiendra donc au responsable du traitement de s'assurer que les mentions légales qui accompagnent la collecte des données à caractère personnel soient clairement visibles. Cela implique donc d'éviter de reléguer ces mentions à des endroits peu accessibles du site. Ce principe de transparence invite également le responsable du traitement a fournir un effort rédactionnel et pédagogique afin que les personnes concernées puissent aisément comprendre les enjeux liés à la collecte de leurs données. Ce droit à une information transparente devra sans doute conduire les entreprises à prévoir une place plus importante pour ces mentions qui souvent étaient diluées dans la documentation.

[127] V. RGPD, consid. 58

B. **La contradiction du droit à une information transparente**

130 On observe une certaine contradiction au sein de ce principe de transparence : l'exigence d'une information complète, exhaustive, va en contradiction avec la volonté de rendre l'information accessible. Les mentions vont s'allonger, alors qu'elles étaient déjà diluées dans la documentation fournie par l'e-commerçant. Il sera difficile de rendre l'information complète et « concise ». Selon certains auteurs, cette exigence d'une information transparence aurait sans doute même l'effet inverse de celui escompté : les mentions d'informations seront tellement complexes, ou tellement simplifiés, qu'elles deviendront soit incompréhensibles, soit inutiles pour les personnes concernées[128]. Aussi, un processus de mise en conformité des formulaires de souscription et des conditions générales de produits ou de services est à envisager dès à présent. Force est de constater que les impacts opérationnels de ces changements sont donc conséquents.

131 Il est légitime de s'interroger sur le choix à opérer par le responsable du traitement : faut-il préférer une information exhaustive au détriment d'une information concise ? Ou, au contraire, une information concise mais non-complète, en ne fournissant au moment de la collecte que les informations « primordiales » et opérant un renvoi pour « *en savoir plus* » ?

132 Les nouveautés relatives aux informations à fournir invitent les responsables du traitement à revoir en profondeur le contenu de leurs formulaires de souscription et des conditions générales d'utilisation ou de vente ainsi que la forme de ceux-ci. Aussi en pratique il conviendra de procéder à la publicité de ces nouvelles mentions, de manière individualisée ou groupée, par exemple en publiant une politique de gestion des données personnelles, sous réserve de s'assurer que l'ensemble des personnes concernées par les traitements y aient accès. On peut s'interroger sur l'effet négatif de cette mesure : au lendemain de l'entrée en application du règlement, le consommateur prendra-t-il le temps de s'informer de tous les changements de politique de collecte des données personnelles des sites sur lesquels il effectue normalement ses achats[129] ?

[128] Pour cet avis : G. Desgens-Pasanau, « RGPD : entre incertitudes et occasions manquées », *Dalloz IP / IT* 2016 p. 335

[129] Chaque personne, en tant que consommateur connait en effet cette alerte « {E-commerçant} a mis à jour ses conditions générales d'utilisation, appuyer ici pour les connaitre ».

133 Cette information reste cependant d'une importance primordiale afin que la personne concernée puisse, à compter de la collecte de ses données, connaître la consistance de ses droits et les exercer en connaissance de cause. Surtout, lorsque le traitement est fondé sur le consentement de la personne concernée, cette information sera le préalable nécessaire à un consentement valable, en connaissance de cause.

SECTION II : Un consentement éclairé sur la base de l'information

134 Le consentement des personnes au traitement de leurs données constitue, avec le droit à l'information renforcée, le bouclier protégeant les personnes concernées d'une exploitation massive et non contrôlée de leurs données, notamment en matière de prospection commerciale et de publicité ciblée. Selon le rapporteur du Parlement européen sur la réglementation de la protection des données, « *le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données* »[130].

135 Avec l'entrée en application du Règlement, le consentement demeure donc un des éléments fondateurs de la licéité du traitement, comme cela est rappelé à l'article 6§1 du Règlement[131]. La consistance de ce renforcement du consentement explicitée (**Paragraphe 1**), permettra de mettre en lumière les incertitudes et craintes qui n'ont pas été réglées par le Règlement (**Paragraphe 2**).

§1 : La consistance du renforcement du consentement

136 Le renforcement du consentement de la personne concernée par le traitement passe tout d'abord par la consécration d'une définition de la notion par le Règlement (**A**). L'édiction de nouvelles règles relatives à la gestion du consentement contribue également au renforcement du consentement (**B**).

[130]Rapport sur la proposition de règlement, Jan Philipp Albrecht, Exposé des motifs, Doc A7-0402-2013 du 21-11-2013

[131] RGPD, art. 6§1 : « *le traitement n'est licite que si et dans la mesure où la personne concernée a consenti au traitement de ses données à caractère personnel, pour une ou plusieurs finalités spécifiques* ».

A. Une notion unifiée à l'échelle européenne

137 La définition donnée par le Règlement (***2***) met fin aux divergences nationales qui avaient pu voir le jour du fait de la nécessaire transposition de la Directive 95/46/CE (***1***).

1. *Une notion antérieure sujette aux divergences*

138 La loi du 6 janvier 1978, dans sa version originelle, ne faisait pas référence au consentement. C'est sous l'influence de la Directive n°95/46/CE que le droit français a intégré la notion de consentement. L'article 2 (h) de la directive n°95/46 définit le consentement comme « *toute manifestation de volonté, libre, spécifique et* ***informée*** *par laquelle une personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». L'article 7 (a) de la directive ajoute que le premier des six motifs justifiant le traitement de données est le consentement « *indubitable* » de la personne concernée, c'est à dire sans ambiguïtés.

139 La transposition de la Directive en droit interne a rendu la notion encore plus obscure, faisant l'objet d'interprétation divergente selon le droit national considéré. Aussi, certains Etats exigent un consentement écrit, d'autres se contentent d'un consentement explicite132. Notamment, la loi Informatique et liberté ne définit pas ce consentement alors même qu'elle autorise les traitements fondés sur le consentement. En effet, l'article 7 de la Loi du 6 janvier 1978 prévoit qu'un traitement de données doit avoir reçu le consentement de la personne concernée ou respecter les conditions fixées à l'article 7[133], mais aucune définition du consentement n'est prévue[134]. A ces divergences s'ajoutent des difficultés pratiques pour apprécier le consentement donné en ligne. Pour exemple, faut-il considérer que les paramètres de navigation expriment le consentement de l'internaute, alors même qu'il ne les aurait pas délibérément choisis ?[135] Une clarification des conditions du consentement est apparue

[132]Sur le fait que la Directive a engendré 27 droits nationaux différents, v. point n°7

[133] Notamment l'article prévoit que le traitement peut être fondé sur le respect d'une obligation légale incombant au responsable du traitement, la sauvegarde la vie de la personne concernée ; l'exécution d'un contrat auquel la personne est partie, etc.

[134] Un auteur estime que de par cette absence de définition, le législateur est resté « fidèle en cela à la tradition législative française exempte de définition » : A. Debet, « La protection des données personnelles, point de vue du droit privée », *Revue droit public*, 01/01/2016 n°1 p. 17

[135] Sur ces questionnements, v. M. Ailincai, « Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel », *R. UE* 2014 p. 170

nécessaire afin qu'il soit donné en toute connaissance de cause.

2. *Le consentement au sens du Règlement*

140 L'article 4 §11 du Règlement définit le consentement comme « *toute manifestation de volonté, libre, spécifique, éclairée et* ***univoque***[136] *par laquelle la personne concernée accepte, par une déclaration ou par acte positif clair, que des données la concernant fassent l'objet d'un traitement* ».

141 Cette définition est plus précise que celle connue sous l'empire de la directive de 1995, et surtout sous l'empire de la loi informatique et libertés, en l'absence de définition. Le Règlement exige un caractère éclairé et univoque du consentement ; et sa manifestation par une déclaration ou par un acte positif clair. Ainsi, une démarche active est donc nécessaire, par opposition à une abstention ou au silence qui ne sauraient ainsi être assimilés à un consentement implicite. Encore convient-il de s'attarder sur les modalités de gestion du consentement.

B. La gestion clarifiée du consentement

142 Le règlement prévoit de nouvelles règles quant aux conditions de recueil du consentement (***1***) ainsi qu'à la possibilité de retirer le consentement au traitement (***2***).

1. *La manifestation du consentement*

143 Le règlement énonce que le consentement peut résulter d'une déclaration ou d'un acte positif clair. Il convient de s'attarder sur la notion d'acte positif clair : dans le cadre de l'e-commerçant la pratique la plus courante est de prévoir une case à cocher (et non pré-cochée)[137]. On peut également envisager comme manifestation de volonté par un acte positif, l'option de la personne concernée « pour certains paramètres techniques pour des services de la société de

[136] La proposition de règlement parlait d'une « manifestation de volonté […] **explicite** », sans doute faut-il regretter la disparition de la notion dans le texte définitif. Pour un tel avis : M. Boizard, « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? » : *CCE* n°3, Mars 2016, étude 6
[137] V. point n°114

l'information »[138], notamment en matière de cookies, afin de se voir proposer de la publicité ciblée. L'acte positif clair peut enfin être représenté par le renseignement des données personnelles de manière volontaire en remplissant le formulaire de collecte.

144 Le consentement doit être donné pour une ou plusieurs finalités conformément à l'article 6§1a) du Règlement, excluant l'application du consentement à une finalité exprimée de manière générale. C'est dire que lorsque les données peuvent être traitées à différentes fins, celles-ci doivent être énoncées à la personne concernée, faute de quoi le traitement pour une finalité qui n'a pas fait l'objet d'une information de la personne ne sera pas valable faute de consentement. Il est possible d'illustrer cette affirmation en prenant l'exemple de la prospection commerciale. La collecte de l'adresse mail pour recevoir une newsletter de la part de l'e-commerçant ne vaut pas acceptation de la personne à recevoir la newsletter des partenaires de l'e-commerçant. Il faut préciser cette finalité au moment de la collecte de l'adresse mail, et cette finalité peut être refusée par la personne concernée. De même, le consentement ne peut pas être recueilli en même temps qu'une autre déclaration ou que l'acceptation des conditions générales ou du contrat conformément à l'article 7§2 du Règlement. Le règlement sous-entend ainsi que l'acceptation des conditions générales d'utilisation ne vaut pas, par exemple, acceptation à faire l'objet de publicité ciblée. Cette finalité étant accessoire à l'objet principal du contrat, il faut recueillir un consentement spécifique pour cette dernière finalité.

145 Cette nécessité de recueillir le consentement finalité par finalité implique une grande clarté ainsi qu'une exhaustivité des finalités, ce afin d'éviter le traitement pour des finalités ultérieures sans l'accord de la personne et surtout afin que la personne concernée retrouve une certaine maitrise de ses données. La problématique du droit à une information transparente se retrouve bien dans la question du consentement au traitement.

146 Enfin dans le cadre de ces nouvelles règles relatives au recueil du consentement, il appartiendra au responsable du traitement de démontrer que la personne concernée a donné son consentement139. Afin de pouvoir gérer cette nouvelle obligation, le responsable du traitement devra avoir recours à des moyens fiables assurant la traçabilité du consentement et l'intégrité du contexte de son recueil, quel que soit le mode de recueil choisi. Aussi, cette nécessité de prouver le consentement donné par la personne concernée au traitement interroge sur les

[138]V. RGPD, consid. 32
[139]RGPD, art. 7§1 sur la preuve du consentement

traitements alors en cours à la date d'entrée en application du règlement. Sans doute, le responsable du traitement devra-il recueillir à nouveau le consentement des personnes concernées par le traitement antérieur à sa mise en conformité avec le règlement afin de pouvoir assurer une traçabilité de leur consentement, et d'être en mesure de prouver leur consentement au traitement.

2. *Le retrait du consentement*

147 La personne aura le droit de retirer son consentement à tout moment et sans avoir à justifier ce retrait[140]. Le retrait ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait et ne s'applique qu'à compter de la date de demande par la personne concernée. La possibilité de retirer son consentement devant faire l'objet d'une information à la personne concernée[141.] Le Règlement précise bien qu'il est aussi facile de retirer son consentement qu'il a été aisé de le donner. Cette possibilité prend acte des difficultés actuelles à retirer son consentement ; voir dans certains cas extrêmes de l'impossibilité de retirer son consentement à défaut d'une procédure permettant ce retrait[142].

148 Le responsable du traitement devra donc revoir son processus interne pour satisfaire à cette nouvelle exigence de faciliter le retrait du consentement. Il faudra notamment intégrer les données de preuve de ce retrait dans son système informatique.

149 Au vu du nombre de contraintes imposées par ce droit à l'information renouvelé, le responsable du traitement pourrait essayer d'invoquer comme fondement du traitement l'intérêt légitime, permettant de faire fi du consentement de la personne concernée. Dans le cadre du e-commerce en effet, le règlement prévoit bien que la prospection commerciale peut constituer un intérêt légitime du responsable du traitement, même si ce fondement est à manier avec prudence[143].

[140]RGPD, art. 7§3: « **Il est aussi simple de retirer son consentement que de donner son consentement** »
[141]RGPD, art. 13§2 c)
[142]Délibération n°2015-155 du 1 juin 2015 prononçant une sanction pécuniaire à l'encontre de la société PRISMA MEDIA
[143] V. points n°75 et suivants

§2 : Les craintes sur la place laissée au consentement

150 Censé être un fondement protecteur pour la personne concernée, la légitimité du consentement au traitement des données peut être discutée (**A**). De même, le fondement juridique que constitue l'intérêt légitime du responsable du traitement laisse craindre de la place restante pour le consentement (**B**).

A. La légitimité du consentement

151 L'étude de la place du consentement dans le Règlement montre qu'il est un véritable marqueur du degré de subjectivisation du droit de chacun sur ses données[144]. Le Règlement ne saurait cependant aller jusqu'à la consécration d'un droit à l'autodétermination informationnelle, pourtant attendu par certains[145]. Le droit à l'autodétermination informationnelle est un principe d'origine jurisprudentielle[146]. Ce droit permet à l'individu de demeurer libre de conduire son existence dans une société qui l'amène à laisser des traces de ses données personnelles. Ce principe assure donc l'autonomie de décision de l'individu, mais il ne s'agit pas d'un droit subjectif : « *il se situe à un autre niveau […] et donne tout son sens aux droits subjectifs [droit d'accès, d'information …] qui tendent à le garantir et doivent être interprétés et mis en lumière de cette finalité* »[147].

152 Force est de constater la place minime du consentement, l'ambiguïté de son rôle au sein du règlement ; et de manière générale dans le traitement des données. Si l'exigence de recueillir le consentement peut traduire un renforcement de la protection des personnes physiques à l'égard du traitement de données les concernant ; cette exigence peut tout autant être conçue comme indolore, étant donné le degré de banalisation auquel il est possible d'arriver en pratique. En effet, comme il a été vu précédemment, il peut s'agir simplement pour l'utilisateur, de cocher une case ou d'approuver des conditions générales qu'il ne lit pas. Aussi, même dans le cas d'un internaute ayant effectué la lecture des informations, si l'internaute refuse les traitements

[144] Notamment, originellement la loi du 6 janvier 1978 ne prévoyait le consentement explicite que pour le traitement des seules données sensibles
[145] N. Martial-Braz, « Le renforcement des droits de la personne concernée », Dalloz IP / IT 2017 p. 253
[146] Première consécration par la Cour fédérale d'Allemagne dans un arrêt du 15 décembre 1983 qui affirme que la constitution garantit « l*a capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ».
[147] Rapp. CE, *Etude annuelle 2014 : le numérique et les droits fondamentaux,* doc. Fr., 2014, p. 267 et s.

projetés par le responsable du traitement, celui-ci peut se voir refuser l'accès au service. Il arrive donc fréquemment une acceptation des conditions d'utilisation du service de par l'incitation créée par un refus d'accès au service.

153 Dans ces hypothèses, le consentement perd de sa légitimité, et deux positions se justifient :

- Faut-il réserver, par conséquent, le consentement aux traitements présentant le plus de dangers pour l'utilisateur, comme le cas d'un traitement de données sensibles ? Et en cas de collecte des autres données, atténuer la prise de conscience des risques engendrés par les traitements ?
- Au contraire, faut-il prévoir un recueil automatique du consentement, avec le risque de banalisation que cela représente ?

Les dispositions de l'article 7 du Règlement ne règlent pas toutes les difficultés pratiques auxquelles l'utilisateur peut se heurter[148]. Un acte délégué d'interprétation du Règlement serait attendu d'ici l'entrée en application du règlement.

B. Le fondement de l'intérêt légitime du responsable du traitement

154 Force est de constater que le consentement, fondement censé renforcer la protection des personnes physiques, n'est qu'un des fondements légitimes du traitement parmi six autres comme cela a été vu précédemment149. Le Règlement propose un autre fondement bien plus puissant et propre à marginaliser le consentement : l'intérêt légitime du responsable du traitement. Ce fondement fait office de véritable « cheval de Troie »[150] de la protection proposée au titre du consentement. Le fondement que constitue l'intérêt légitime peut réellement constituer une manœuvre aux fins d'écarter le consentement de la personne concernée. En effet, qu'est-ce qu'un intérêt légitime ? Ne risque-t-on pas avec ce fondement d'autoriser tout traitement effectué par une société commerciale, en ce qu'il est légitime pour une telle entreprise de rechercher un intérêt économique dans les traitements de données de ses utilisateurs ?

[148] Sur ce point de vue : N. Martial-Braz, « Quel avenir pour la protection des données à caractère personnel en Europe ? » *D.* 2013 p. 2788
[149] V. point n°75
[150] Ibid.

155 En l'absence de consentement, le règlement développe le droit d'opposition au traitement. Notamment, dans le cas d'un traitement fondé sur l'intérêt légitime du responsable du traitement pour la prospection commerciale, le Règlement prévoit le droit pour la personne concernée de s'opposer à ce traitement, sans frais[151]. Au vu de la puissance du fondement que constitue l'intérêt légitime du responsable du traitement, il faut espérer que sa force, et la possible désuétude du consentement, soient contrebalancées par ce réel renforcement du droit d'opposition.

156 Le Règlement renforce donc, textuellement parlant du moins, les droits des personnes concernées préalablement à la collecte de leurs données. Aussi, aux fins de rendre la maitrise des individus quant à leurs données, l'outils règlementaire renforce les droits des personnes concernées par le traitement à compter de la collecte. En effet, à compter du traitement de ses données, la personne concernée peut exercer les droits portés à sa connaissance préalablement au traitement.

[151]RGPD, art. 21§2

CHAPITRE II : LE RENFORCEMENT DES DROITS POSTERIEUREMENT A LA COLLECTE DES DONNEES

157 Au-delà du renforcement des droits préexistants dont le droit à l'information et de rectification, c'est en reconnaissant de nouvelles prérogatives en faveur des personnes concernées que se traduit véritablement le renforcement de la protection des droits des personnes physiques. Le Règlement consacre de nouveaux droits dont un droit à l'oubli[152]. Ce droit permet à la personne de faire cesser la diffusion de données la concernant, qu'elle juge préjudiciable à son égard. Le Règlement note que « ce droit est pertinent, en particulier, lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données (...) »[153]. Ce droit à l'effacement trouvera sa raison d'être dans le secteur des réseaux sociaux[154].

158 Outre ce droit à l'effacement, le règlement consacre un nouveau droit à la portabilité des données. La consécration de ce droit a pour objectif de parachever le renforcement de la protection des personnes physiques à l'égard de leurs données. Il convient d'analyser la mise en œuvre de ce droit à la portabilité (**Section I**). L'analyse de cette mise en œuvre, sous tous ses angles, permettra de se questionner sur la réelle portée de ce nouveau droit (**Section II**).

SECTION I : La mise en œuvre du droit à la portabilité

159 La mise en œuvre du droit à la portabilité recouvre deux idées. La première idée consiste à s'intéresser aux modalités d'intégration du concept de portabilité au sein du Règlement (**Paragraphe 1**). La deuxième idée revient à analyser les modalités concrètes d'exercice du droit à la portabilité par la personne concernée (**Paragraphe 2**).

[152]RGPD, art. 17
[153] RGPD, consid. 65
[154] Pour une analyse détaillée de ce droit à l'oubli dans le cadre des réseaux sociaux, v. M. Boizard, « Facebook forever : les réseaux sociaux peuvent-ils être contraints de nous oublier ? »*: CCE* n°4, Avril 2015, étude 7

§1 : La consécration d'un droit à la portabilité des données

160 La notion de portabilité, bien que nouvelle dans le cadre de la protection des données à caractère personne (**B**), n'est pas moins déjà connue dans le cadre de certains services (**A**).

A. De la portabilité des services

161 Le dictionnaire Larousse définit la portabilité comme « l'aptitude d'un programme informatique ou d'un progiciel à être exécuté, sans grande modification, sur des ordinateurs de types différents ». A titre d'illustration, il existe la portabilité du numéro de téléphone[155], qui permet de changer facilement d'opérateur de téléphonie mobile, et ce en conservant le numéro de téléphone originel, encore appelée la conservation du numéro. D'autres services permettent ce transfert d'un service à un autre et renvoie ainsi au concept de portabilité, alors même qu'ils n'en portent pas le nom. Tel est le cas pour le changement de fournisseur d'électricité ou de gaz, de banque[156]. Ces changements peuvent être opérés facilement et à moindre coût.

162 En somme, le concept de portabilité réside dans la possibilité pour le consommateur de transférer un service d'un fournisseur à un autre sans pénalisation d'ordre technique ou financier. De la sorte, le concept de portabilité s'analyse bien en une prestation de services. Force est de constater qu'un nombre encore trop insuffisant d'utilisateurs de service, et de consommateurs d'une manière générale, profitent de ces opportunités de changer de fournisseur. Si les services peuvent être « portés » d'un fournisseur à un autre, les données à caractère personnel pourraient sans problème être portées[157]. Le Règlement ne fait qu'élargir et formaliser cette possibilité, sans la circonscrire aux services mobiles.

[155] C. post. Comm. Électr., art. D406-18 et D406-19

[156]Encore que la consécration d'une portabilité dans le secteur bancaire dans le Règlement normalise plus encore cette possibilité de transférer ses comptes d'une banque à une autre.

[157]Pour un tel avis, P.-N. Schwab, *RGPD : qu'est-ce que le concept de portabilité des données ?* [en ligne] Into the minds, 14 juin 2017
Disponible sur : < http://www.intotheminds.com/blog/?s=portabilit%C3%A9>

B. A la portabilité des données

163 La portabilité des données est une suite naturelle à la portabilité des services. Le concept est donc introduit dans le Règlement (***1***), Le législateur français a, à tort ou à raison, anticiper le droit à la portabilité ; il convient d'étudier l'articulation entre les textes (***2***).

1/ L'introduction du concept dans le Règlement

164 Avant son adoption définitive, le droit à la portabilité des données a été l'objet de vives discussions et désaccords. La portabilité, telle que proposée par la Commission européenne, a fait l'objet de nombreux commentaires. Pour exemple, la Chambre de commerce et d'industrie de la région Paris Ile-de-France a pris position sur cette proposition le 14 février 2013, et estimait que l'article posait de nombreux problèmes, notamment en ce qu'il permettait une transmission de données à d'éventuels concurrents. D'autres risques ont peu être avancés par la possibilité de porter les données d'un service à un autre, notamment les risques d'une usurpation d'identité. Ces risques sont contradictoires avec une volonté de renforcer la protection des personnes physiques à l'égard des données à caractère personnel. Le Parlement européen, dans sa résolution législative du 12 mars 2014 sur la proposition de règlement, avait même supprimé l'article 18[158] de la proposition de Règlement.

165 Conformément à l'article 20 paragraphe 1 du Règlement, les personnes concernées ont « *le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* ». Conformément au paragraphe 2, la personne concernée a également le droit d'obtenir que les données soient transmises directement d'un responsable du traitement à un autre, « lorsque cela est techniquement possible ». Ce droit comporte donc deux volets :

[158]Correspond à l'actuel article 20 du Règlement

- le droit de récupérer, sous certaines conditions, des données à caractère personnel concernant une personne
- le droit de demander au responsable du traitement de les transmettre à un autre responsable et directement

166 Pour illustrer de manière pratique la notion de portabilité et son application dans le cadre du e-commerce, l'exemple peut être pris d'un utilisateur d'un service d'écoute de musique en streaming payant. Avec ce nouveau droit à la portabilité, ce même utilisateur pourra très bien récupérer les données le concernant et même demander le transfert de ses données à un nouveau prestataire.

2/ L'anticipation du concept en droit interne

167 Le législateur français a souhaité anticiper l'entrée en application du Règlement européen par la loi pour une République numérique[159]. Le succès de l'introduction prématuré de ce droit, et de la loi pour Une république numérique en général, est mitigé. Outre la consécration d'un droit à l'oubli numérique, la loi pour une République numérique consacre un « droit à la portabilité et à la récupération des données ».

168 Ce droit à la portabilité et à la récupération des données est prévu par l'article 48 de la loi et ne vise que les données détenues par les fournisseurs d'un service de communication au public en ligne, et ne concerne que les données « autres que personnelles ». Un renvoi est effectué au règlement pour les données à caractère personnel. Les données concernées par la loi sont finalement peu nombreuses. Il s'agira des données constituées par des « fichiers mis en ligne » ainsi que de toutes les données résultant de l'utilisation d'un « compte utilisateur et consultable en ligne ». Cette loi est désormais applicable, mais l'on peut être soulagé de ce que les dispositions relatives à la portabilité et à la récupération des données ne le seront qu'à compter de mai 2018. Une application immédiate aurait conduit à moins bien protéger les données à caractère personnel que les autres données du fait de l'entrée en application du Règlement en mai 2018[160].

[159]L. n°2016-1321 du 7 oct. 2016 pour une République numérique
[160]Sur cet opinion, v. N. Martial-Braz, « Les nouveaux droits consacrés par la loi pour une République numérique – Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP / IT* 2016 p. 525

169 La portée de ce droit est assez incertaine, l'exclusion des données à caractère personnel de son champ d'application risque de réduire à néant l'intérêt de la portabilité, dans la mesure où l'utilisation de la plupart des services de communication en ligne implique le traitement de données à caractère personnel des utilisateurs. L'adoption de ce texte a été fortement critiquée, notamment par l'Association française des Editeurs de Logiciels et Solutions Interne et la FEVAD, qui avait demandé à ce que le droit à la portabilité soit renvoyé au Règlement, afin de ne pas pénaliser la compétitivité des entreprises françaises par rapport à leurs concurrents européens.

170 La juxtaposition de ces deux dispositions, qui risquent de s'enchevêtrer ne sera sans doute pas aisée. Si la superposition de deux droits à la portabilité n'était pas suffisante, une proposition de directive « sur certains aspects des contrats de fourniture de contenu numérique » du 9 décembre 2015 vient prévoir un droit de récupération des données par suite de l'utilisation d'un contenu numérique, au profit du consommateur, en cas de résiliation du contrat[161]. Cette proposition de directive trouve à s'appliquer « à tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur (…) en échange duquel un prix doit être acquitté ou une contrepartie non pécuniaire, sous la forme de données personnelles ou de toutes autres données, doit être apportée de façon active par le consommateur ». Ainsi, trois droits à la portabilité trouveraient à s'appliquer à diverses situations qui pourraient se recouper entre elles. En effet, si la segmentation de la règlementation selon la nature personnelle ou non des données permet d'attribuer l'applicabilité des dispositions du Règlement ou au Code de la consommation, la distinction n'est plus entre la proposition de directive et le Règlement. Et ainsi, dans le cas où la portabilité s'exercerait à compter de la résiliation du contrat, il n'y a pas forcément lieu à favoriser l'application du projet de directive qui a une conception plus patrimoniale de la donnée que celle du règlement[162].

171 Concernant le droit à la portabilité consacré par le Règlement, celui-ci a été clarifié par le Groupe de l'article 29 dans ses lignes directrices[163]. De par sa nouveauté, le thème de la portabilité faisait partie des thèmes identifiés par l'article 29 comme méritant une clarification avant l'entrée en application du règlement[164].

[161] Proposition de directive, article 13
[162] C. Berthet, C. Zolynski, N. Anciaux, al., « Contenus numériques, récupération des données et empouvoirement du consommateur », *Dalloz IP / IT* 2017 p.29
[163]G29, Guidelines on the right to data portability annex, WP242, 13 déc. 2016
[164]Les autres thèmes ayant fait l'objet de lignes directrices étant le délégué à la protection des données et l'autorité chef de file

§2 : Les modalités d'exercice du droit à la portabilité

172 L'article 20 du Règlement conditionne fortement l'exercice du droit à la portabilité. Outre le fait qu'il ne puisse s'effectuer que lorsque le traitement est fondé sur le consentement de la personne concernée sur l'exécution d'un contrat[165], le droit à la portabilité ne sera possible que si le transfert d'un responsable du traitement à un autre est techniquement possible (**A**). Surtout, les données concernées par la portabilité viennent nettement limiter le volume de données pouvant être « portées » (**B**).

A. La faisabilité du transfert de données

173 Outre le cas où la personne titulaire du droit souhaite simplement récupérer ses données, il est possible d'opérer le transfert d'un responsable du traitement à un autre. Dans ce cas, quelles sont les méthodes préconisées pour passer d'un service à un autre ? A défaut de précision dans le Règlement, le Groupe de l'article 29 préconise la mise à disposition d'outils de portabilité sous forme d'interfaces de programmations applicative (API), permettant le téléchargement direct des données par les personnes concernées ainsi que leur transfert direct à un autre responsable du traitement. Une interaction de la personne est ainsi nécessaire dans cet exemple.

174 Le règlement conditionne le droit à la portabilité à la faisabilité technique du transfert. Or, les lignes directrices du Groupe de l'article 29 ne semble pas reconnaître de limites à la mise en œuvre du transfert direct. Le Groupe de l'article 29 invite les responsables du traitement à réfléchir aux moyens permettant le transfert des données. Notamment, lorsque le volume des données rend problématique la transmission des données via internet, il serait possible d'envisager des solutions alternatives comme l'envoi de contenu « en direct » ou l'enregistrement des données sur des supports de stockage (CD, DVD, etc.) permettant à la personne concernée de transmettre directement les données à un autre responsable du traitement. Cette technicité dans le transfert ne sera-t-elle pas décourageante pour l'utilisateur désirant porter ses données d'un service à un autre ?

[165]Le droit à la portabilité est exclu lorsque le fondement de la collecte est l'exécution d'une mission d'intérêt public. La référence au traitement basé sur l'intérêt légitime du responsable du traitement est totalement absente du texte ; on peut donc légitimement se questionner sur la possibilité, ou non, de porter les données collectées en vertu de ce fondement ; et, encore une fois, sur la force de ce fondement juridique.

175 De même, et non spécifiquement à la portabilité, l'exercice des droits doit s'effectuer de manière gratuite. Une exception à cette gratuité est prévue en cas de demande excessive ou infondée, notamment en raison du caractère « répétitif » de la demande. La difficile faisabilité du transfert ne sera-t-elle pas mise en avant par le responsable du traitement destinataire d'une telle requête ? De par le silence du Groupe de l'article 29 sur ce point, il ne semble pas que le fait de répondre à des demandes de portabilité des données soient considérées comme une charge effective pour le responsable du traitement. L'organe institué par la Directive de 1995 recommande simplement de définir un délai raisonnable de traitement de la demande et de le communiquer aux personnes concernées.

B. La limitation des données portées

176 L'article 20 du Règlement limite le type de données pouvant être portées d'un responsable du traitement à un autre. Les données doivent en effet concerner la personne titulaire du droit à la portabilité (***1***), et aussi avoir été fournies par la personne concernée (***2***).

1. Des données relatives au titulaire du droit

177 En principe, une personne concernée ne peut exercer son droit à la portabilité qu'à l'égard des données à caractère personnel la concernant. Les lignes directrices déjà mentionnées suggèrent d'assouplir cette limitation, en considérant que le droit à la portabilité peut trouver à s'appliquer pour des données de personnes physiques tierces communiquées par la personne concernée[166]. Le G29 vise expressément l'exemple les contacts téléphoniques, ou les contacts sur un réseau social.

178 L'entorse faite au principe tel que présent dans l'article 20 est conditionnée à ce que les données de personnes physiques tierces restent sous le contrôle du titulaire du droit à la portabilité, et qu'elles ne soient utilisées que pour les besoins personnels ou domestiques du titulaire. Pour s'assurer que l'exercice du droit à la portabilité ne porte pas atteinte aux droits et libertés de tiers, comme cela est prévu à l'article 20,4°, le groupe de l'article 29 préconise

[166]WP242, p. 8

l'interdiction pour le responsable du traitement qui reçoit les données de les utiliser pour de la prospection commerciale[167]. L'entreprise recevant les données est limité quant à l'usage de ces données : il ne peut les utiliser que pour la fourniture du service demandé par le titulaire du droit à la portabilité.

179 **U**ne telle interprétation des données pouvant être « portées » est compréhensible : sans cette possibilité, le droit à la portabilité serait privé de son intérêt principal qui est de faciliter le changement de prestataire et d'éviter ainsi les phénomènes de verrouillage.

2/ Des données fournies par le titulaire du droit

180 Tous les traitements ne sont pas concernés par le droit à la portabilité. Il résulte de l'article 20 que le droit à la portabilité ne s'applique qu'aux traitements automatisés[168] et seulement aux données ayant été « fournies » par la personne concernée. Une lecture stricte pourrait revenir à considérer que seules les données volontairement communiquées par la personne concernée puissent faire l'objet de la portabilité. En effet, l'article ne semble viser que les données dites déclaratives comme, par exemple, les données d'identification ou les données concernant le profil, les préférences saisies par l'utilisateur dans un formulaire au moment de la création d'un compte.

181 Le groupe de l'article 29 opte, là encore, pour une interprétation large de l'exercice du droit à la portabilité, en incluant également les données d'observation, c'est-à-dire les données générées et collectées du fait de l'activité de l'utilisateur. Cela vise notamment les données de trafic générées par les cookies et les traces d'activités. Seules seraient exclues de ce droit les données déduites, comme celles qui découlent de l'analyse des données déclaratives ou des données d'observation. Cela vise les données de profilage qui résultent bien d'un enrichissement effectué par le responsable du traitement. Sur ce point, les lignes directrices du G29 ne sont pas forcément éclairantes. En effet, dans le cas du profilage, notamment à des fins de prospection commerciale, le fondement juridique de la collecte n'est-il pas l'intérêt légitime du responsable du traitement, fondement ne permettant pas l'exercice du droit à la portabilité ? La mise en œuvre de ce droit à la portabilité, mise en œuvre textuelle et pratique, n'est donc pas aisée. La

[167]WP242, p. 9
[168]Excluant ainsi les fichiers manuels de traitement de données

portée que le Règlement a voulu conférer au concept de portabilité n'aurait-t-il pas fait obliger aux rédacteurs du texte la faisabilité du mécanisme ?

Section II : La portée du droit à la portabilité

183 Si le droit à la portabilité a pour enjeu premier de conférer aux individus une plus grande maitrise de leurs données (**paragraphe 1**) ; cette portée peut être discutée et doit être mis en balance par d'autres enjeux induits par ce droit (**paragraphe 2**).

§1 : Une maitrise sur le traitement opéré

184 L'étude de la consistance du droit à la portabilité permet de mieux comprendre en quoi ce droit est destiné à renforcer le contrôle exercé par les personnes concernées sur leurs propres données. Le droit à la portabilité permet de demander au responsable du traitement de transférer directement les données à un autre responsable du traitement, sans que ce dernier ne puisse s'y opposer. Cela permet donc d'éviter la dépendance, le blocage au sein d'un service pour le consommateur.

185 La mise en œuvre de ce droit par le consommateur va permettre aux individus de ne pas se retrouver bloquer dans un système captif. En effet, il ne faut pas que la volonté de changer, notamment, de fournisseur d'un service soit réduite à néant du fait de la peur de perdre ses données. Jusqu'à maintenant en effet, la perspective de devoir abandonner ses données en cas de changement de services, ou de devoir se lancer manuellement dans une récupération des données générées peut être décourageante et mettre un terme à la volonté de changer d'entreprise. La mobilité et ainsi le choix du consommateur vont clairement être renforcer par la possibilité de recevoir du responsable du traitement les données à caractère personnel dans le format imposé par le Règlement[169].

[169]Sur l'idée que la portabilité est la conséquence d'une revendication d'une limitation des « barrières à la sortie », v. A. Ancieux et J. Farchy, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue Internationale de Droit Economique*, 2015/3 (t. XXIX) p. 307. 338

186 Le droit à la portabilité s'inscrit bien dans la logique « d'empouvoirement » des individus et de rééquilibrage des rapports de forces entre les responsables de traitements et les consommateurs. Cette reprise du contrôle tend également à se généraliser, de par la future entrée en vigueur de la loi pour une République numérique, le projet de directive sur le contenu numérique, et aussi et surtout par la proposition de Règlement renforçant la protection de la vie privée des personnes physiques.

187 Le droit à la portabilité s'inscrit bien dans cette logique. Afin de garantir l'effectivité du droit à la portabilité, les responsables de traitement devront ainsi prévoir des formats de traitements interopérables et génériques, de sorte à ce que les données puissent être communiquées sans difficulté à un autre responsable du traitement. La reconnaissance de ce droit sera lourd de conséquences pour les entreprises qui devront mettre en place des mécanismes autorisant et permettant l'extraction des données relatives à un individu :

- les nouveaux projets devront prendre en compte, dès l'origine, la possibilité d'assurer la portabilité des données[170]
- Encore plus complexe, le responsable du traitement devra revoir et adapter les systèmes informatiques existants pour qu'ils soient en conformité avec ce nouveau droit accordé aux individus.

188 La force du droit à la portabilité ne saurait cependant être absolue. Premièrement, cette force est, pour l'heure, simplement textuelle. Ensuite, l'analyse de l'article 20 du Règlement et des lignes directrices du Groupe de l'article 29 atteste de ce que sa mise en œuvre reste encore sombre, surtout que trois droits à la portabilité seraient susceptibles de s'appliquer aux mêmes traitements de données. D'autres éléments permettent de conclure, pour l'heure, à une portée limitée du droit à la portabilité.

[170]Conformément à l'obligation de mettre en place une stratégie de gouvernance des données, et particulièrement l'obligation de protection des données dès la conception et par défaut point n°41 et suivants

§2 : Une maitrise nuancée

189 Cette vision idéaliste du droit à la portabilité, constituante d'un véritable renforcement de la protection des personnes physiques à l'égard des traitements de données les concernant, est à relativiser. La nature réelle de ce nouveau droit sera révélée à compter de l'entrée en application du Règlement. En effet, la portée de ce droit peut être nuancée en ce que le droit à la portabilité ne constituerait, en somme, qu'un substitut du droit d'accès, plus limité (**A**). Surtout, ce droit à la portabilité a également un objectif économique, consistant en la libre circulation des données (**B**).

A. Un droit d'accès limité

190 Ce droit à la portabilité des données peut être considéré comme le prolongement de l'actuel droit d'accès de l'individu aux données à caractère personnel le concernant[171]. En effet, le droit d'accès et à la portabilité visent tous deux à renforcer le contrôle exercé par les personnes sur leurs données à caractère personnel. Les deux droits permettent à la personne concernée d'avoir accès aux données la concernant.

191 Le droit d'accès est présenté à l'article 15 du Règlement, et offre la possibilité pour la personne concernée d'obtenir du responsable du traitement la confirmation que des données la concernant sont traitées. Lorsque tel est le cas, la personne concernée a le droit d'obtenir du responsable du traitement l'accès à ces données, et surtout, l'accès à certaines informations ; notamment :

- les finalités du traitement,
- les catégories de données concernées,
- les destinataires des données,
- la durée de conservation des données,
- l'existence d'un profilage et des informations utiles concernant la logique sous-jacente

[171]En ce sens : Résolution législative du Parlement européen sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personne et à la libre circulation de ces données du 10-6-2014, p.2

192 L'étude des conditions d'applicabilité de ces deux droits met bien en évidence le fait que le droit à la portabilité – plus que de constituer un prolongement du droit d'accès, constitue plutôt un droit d'accès limité. Ainsi, alors que le droit d'accès concerne tous les traitements, le droit à la portabilité ne vise que les traitements automatisés et fondés sur le consentement ou sur le contrat. Surtout, alors que le droit d'accès concerne toutes les données, le développement sur le droit à la portabilité montre que cette portabilité ne s'applique qu'aux données concernant la personne titulaire du droit et communiquées par elle, et non pas notamment sur les données déduites172.

193 Enfin, les conditions d'exercice du droit d'accès sont plus avantageuses et mieux établies que le droit à la portabilité. Alors que le droit d'accès doit s'exercer dans un mois à compter de son exercice, aucun délai spécifique n'est prévu pour le droit à la portabilité. Cela peut sans doute être justifié de par la nouveauté du dispositif qui contraint les entreprises à l'adoption de nouvelles mesures.

194 Surtout, l'article 15 paragraphe 3 permet à la personne concernée par le traitement d'exiger du responsable du traitement une copie des données faisant l'objet du traitement. Cela n'est-il pas semblable à la possibilité offerte par le droit à la portabilité de récupérer ses données ? Aussi, au vu des contraintes imposées pour le droit à la portabilité, ne vaut-il pas mieux exercer son droit d'accès, obtenir une copie des données, et clôturer le compte d'utilisateur afin de mettre un terme au traitement ? Le droit à la portabilité n'aurait d'intérêt qu'en cas de volonté de transférer des données d'un responsable du traitement à un autre.

195 La question se pose aussi de l'intérêt pratique du droit à la portabilité. Si la portabilité trouve un intérêt certain dans des domaines tels que la banque ou l'assurance ; où le cloisonnement auprès d'une entreprise ne devrait pas être autorisé, dans la mesure où des données sensibles trouvent à être traitées ; dans le cas d'un e-commerçant l'opportunité d'un droit à la portabilité apparaît restreinte. En effet, une fois que l'utilisateur a récupéré ses données, que peut-il bien faire de celles-ci ? En effet, le Règlement et le Groupe de l'article 29 n'indiquent pas de standard dans la transmission de ces données. Ainsi, il n'est pas assuré que le responsable du traitement puisse tirer un quelconque avantage des données transmises. Pour exemple, la récupération de l'historique d'achat d'un hypermarché afin de les porter à un autre

[172]v. point n°181

hypermarché risque de présenter un intérêt limité : les systèmes informatiques des deux e-commerçants sont probablement différents et non compatibles entre eux.

196 Cette comparaison entre droit d'accès et droit à la portabilité semble montrer qu'en termes d'objectif de protection, le droit d'accès l'emporte. Aussi, il est opportun de s'interroger sur la portée consumériste de ce droit.

B. Un droit consumériste

197 Le propos a déjà été avancé[173] lorsqu'il a été question d'analyser le droit à la portabilité comme une manière d'éviter les barrières à la sortie d'un service. Cet logique de reprise de contrôle sur ses données, ne s'inscrit pas tant dans une logique de protection des données, mais plutôt dans l'optique de pouvoir librement changer de prestataire, et ainsi de faire jouer la concurrence sur le marché. Il est ainsi possible d'analyser le droit à la portabilité sous un autre angle que celui de la protection des données. En effet, le droit à la portabilité semble d'avantage reconnu dans une perspective commerciale et concurrentielle que dans une perspective de protection de la vie privée et des données de l'individu.

198 Plus qu'un droit de la personnalité corollaire du droit d'accès, le droit à la portabilité est un droit essentiellement consumériste, dont la raison d'être est de favoriser le jeu de la concurrence et de permettre l'émergence de nouveaux services[174]. Cette nature du droit à la portabilité ne peut qu'être attestée du fait de la consécration du droit à la portabilité français dans le Code de la consommation.

199 Mais n'est-ce pas là l'autre pendant du Règlement général sur la protection des données, assurer la libre circulation des données à caractère personnel des personnes physiques ?

[173]V. point n°186

[174]Pour cette vision plus consumériste du droit à la portabilité, v. N. Metallinos, « La protection des données au service de l'émancipation du consommateur », *CCE* n°2, Février 2017, comm. 17

CONCLUSION

200 L'étude réalisée sur le renforcement de la protection des données personnelles opéré par le Règlement, dans le cadre d'opérations de commerce électronique, montre que ce renforcement sera effectif de part un rehaussement des obligations de l'e-commerçant et des droits du consommateur. La réalité de ce renforcement de protection peut cependant être discuté : difficulté à mettre en œuvre les principes textuelles, utopie de certains de ces principes. Aussi, il peut être argué de l'égalité des responsables de traitement dans le cadre du Règlement, s'il est opportun de renforcer significativement les obligations d'entreprises traitant massivement les données à caractère personnelles de millions d'individus, le cas des moyennes et petites entreprises doit être souligné. Pensons à la start-up proposant des solutions innovantes autour de la donnée, la mise en conformité avec le Règlement sera-t-elle aisée ?

201 Une lecture attentive du Règlement atteste de ce que le renforcement de la protection des données s'opèrera par un encadrement de l'activité des responsables de traitements, et d'un rehaussement de leurs obligations. En effet, dans l'octroi de nouveaux droits ou le renforcement des droits existants, le Règlement encadre largement le traitement de données à caractère personnel et astreint les entreprises à de nombreuses contraintes.

202 Enfin, il ne faut pas oublier pas que le Règlement porte sur la protection des personnes physiques à l'égard du traitement de leurs données, mais également sur la libre circulation de ces données. Voilà le deuxième objectif du Règlement : une libre circulation des données au sein de l'Union européenne et la consolidation d'un marché numérique. Il ne faut pas omettre que doit être mis en balance la protection des données et d'autres intérêts divergents : droit des tiers, libertés fondamentales – telle la liberté de circulation des données. Les enjeux sont tels que l'adoption du texte définitif a souffert du lobbying extrême de la part des grandes entreprises, surtout non européennes, que sont Google, Facebook et Appel. La réalisation de ces objectifs n'est-elle pas cependant antinomique ? La volonté de consolider un marché numérique ne revient-t-il pas à considérer la donnée personnelle comme un bien dans le commerce ; rendant illusoire la consécration d'un droit personnel, subjectif sur ces données, en tant qu'attribut de la personne ?

203 Un compromis peut être trouvé. La juxtaposition de ces deux objectifs peut être synthétisé de la sorte : le but du règlement est de créer de la confiance pour les personnes concernées – en renforçant leurs droits- sans pour autant mettre un frein à l'activité économique et au développement des entreprises européennes. Autrement dit, l'accru de protection, et l'encadrement des traitements a pour dessein de renforcer la confiance des consommateurs dans les services en ligne ; cette confiance accordée va donner un regain à la croissance, à l'emploi et à l'innovation en Europe.

204 Force est de constater que le sujet complexe et d'actualité des données à caractère personnel met en balance deux droits fondamentaux : le droit fondamental à la protection des données et le droit fondamental à la libre circulation de ces données.

BIBLIOGRAPHIE

OUVRAGES :

- Académie des technologies, *Big data : un changement de paradigme peut en cacher un autre,* 1e Ed., EDP Sciences, 2016
- Bensoussan, A., *Règlement européen sur la protection des données – textes, commentaires et orientations pratiques,* 1e éd., Larcier, coll. Lexing – Technologies avancées & droit, 2016
- Eynard, J., *Les données personnelles, quelle définition pour un régime de protection efficace* ? : Michalon, 2013
- Haas, G., *Guide de l'e-marketing*, ENI Collection, coll. Data pro, 2013
- Haas, G., *Guide juridique de l'e-commerce et de l'e-marketing*, ENI Collection, coll. Data pro, 2015
- Mattatia, F., *Traitement des données personnelles : le guide juridique*, Eyrolles, 2013
- Mattatia, F., *Le droit des données personnelles : n'attendez pas que la CNIL ou les pirates vous tombent dessus !* : 2e Ed., Eyrolles, 2016

ARTICLES, ETUDES ET CHRONIQUES :

- AILINCAI, M., « Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel », *Revue de l'Union européenne*, 2014 p. 170
- ANCIEUX, A., FARCHY, J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », *Revue internationale de Droit économique,* 2015/3 (t. XXIX) p. 307 338
- BANCK, A., « GDPR et sous-traitance : un nouveau devoir de conseil ? », *Dalloz IP/IT* 2017 p.36
- BERTHET, C., ZOLYNSKI, C., ANCIAUX, N., « Contenus numériques, récupération des données et empouvoirement du consommateur », *Dalloz IP / IT* p. 29

- BEYNEIX, L., « Le traitement des données personnelles par les entreprises : big data et vie privée, état des lieux », *La Semaine Juridique Edition Générale*, n°46-47, 9 nov. 2015, doctr. 1260
- BOIZARD, M., « Facebook forever : les réseaux sociaux peuvent-ils être contraints de nous oublier ? »*: Communication Commerce électronique* n°4, Avril 2015, étude 7
- BOIZARD, M., « Le consentement à l'exploitation des données à caractère personnel : une douce illusion *? »*, *Communication Commerce électronique* n°3, mars 2016, étude 6
- BOULET, L. et FROSSARD, L., « Un an de droit de la publicité », *Communication Commerce électronique*, n°7-8, chron. 9
- CAVOUKIAN, A., Information and Privacy Commisionner of Ontario, *Privacy by Design – The 7 foundational principles,* Canada, mai 2010
- CAPRIOLI, E.-A., « Données à caractère personnel et sécurité - notification des violations de données à caractère personnel », *Communication Commerce électronique* n°2, déc. 2011, comm. 116
- COSTES, L., « La Cnil facilitatrice de l'évolution numérique », *Revue Lamy Droit du numérique*, n°136, 1e avril 2017
- DARY, M., « Privacy by Design : un principe de protection séduisant mais complexe à mettre en place », *Dalloz IP/IT* 2016 p. 476.
- DEBET, A., « La protection des données personnelles, point de vue du droit privé », *Revue de droit public*, 01/01/2016 n°1 p.17
- DEBET, A., « Les nouveaux instruments de conformité », *Dalloz IP / IT* 2016 p. 592
- DESGENS-PASANAU, G., « RGPD : entre incertitudes et occasions manquées », *Dalloz IP / IT* 2016 p. 335
- GABRIE, E., « Les pouvoirs des autorités de protection des données », *Dalloz IP / IT* 2017 p. 269
- GHEORGHE-BADESCU, I., « Le nouveau règlement général sur la protection des données, quoi de neuf ? », *Revue de L'Union européenne*, 2016 p. 466

- GODEFROY, L.-D., « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », *Recueil Dalloz* 2016 p. 438
- HAAS, G., « Confidentialité et protection des données », *Dalloz IP/IT* 2017 p. 322
- JOUFFIN, E. et LEMARTELEUR, X., « Du psautier de Mayence au zettaoctets – quel environnement pour le big data ? », *Banque et droit* 2016 n°166 p. 12
- JOUFFIN, E., LEMARTELEUR, X. et GIBON, M.-N., « Le règlement sur la protection des données : les 10 commandements à connaitre pour passer de la théorie à la pratique », *Revue de Droit bancaire et financier* n°4, Juillet 2016, étude 18
- 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
- MARTIAL-BRAZ, N., « Quel avenir pour la protection des données personnel en Europe ? », *Recueil Dalloz* 2013 p. 2788
- MARTIAL-BRAZ, N., « Les nouveaux droits des individus consacrés par la loi pour une République numérique. Quelles innovations ? Quelle articulation avec le Règlement européen ? », *Dalloz IP / IT* 2016 p. 525
- MARTIAL-BRAZ, N., « Le renforcement des droits de la personne concernée », *Dalloz IP / IT* 2017 p. 253
- MAXWELL, W., « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP / IT* 2016 p. 123
- METALLINOS, N., « 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
- METALLINOS, N., « La protection des données au service de l'émancipation du consommateur », *Commerce Communication électronique* n°2, février 2017, comm. 17
- SCARAMOZZINO, E., « Le profilage encadré pour favoriser la diversité culturelle », *Juris art etc.* 2016, n°36, p.6
- VIVANT, M., « Bilan 2016 du e-commerce en France : le cap des 70 milliards a été franchi », *Revue Lamy Droit de l'immatériel* n°134, 1e février 2017

LEGISLATION ET JURISPRUDENCE :

- Code de la consommation
- Code des postes et communications électroniques
- Cour d'appel de Paris, pôle 5, 1re ch., 14 avril 2010, Omar S., Fred T., et a. c/ Sté Daily Motion, RLDI 2010/62, n°2034 p. 47 note R. Har-douin
- Directive n°95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communication électronique)
- L. 6 janvier 1978 : loi Informatique et Libertés
- L. 21 juin 2004 : loi pour la confiance dans l'économie numérique ; dite LCEN
- L. 7 octobre 2017 : loi pour une République numérique
- Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenu numérique (COM/2015/634 final) du 9 décembre 2015
- Proposition de règlement du Parlement européen et du Conseil concernant la protection de la vie privée dans le secteur des communications électroniques, et abrogeant la directive 2002/58/CE (Règlement sur la vie privée et communication électronique) (COM/2017/10 final) du 10 janvier 2017
- Règlement UE/2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Traité sur le Fonctionnement de l'Union Européenne

RECOMMANDATIONS :

- Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions, *Une stratégie pour l'Europe,* 19-5-2010, COM (2010) 245 final

- Avis n°4/2010 du 13 juillet 2010 sur le code de conduite européenne de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct, Groupe de travail « article 29 » sur la protection des données (G29, WP 174)

- Avis n°3/2010 du 13 juillet 2010 sur le principe de responsabilité, Groupe de travail « Article 29 » sur la protection des données (G29, WP 173)

- Lignes directrices régissant la vie privée, et les flux transfrontalières de données à caractère personnel, Organisation de Coopération et de Développement Economiques, 1980 révisées en 2013

- *Rapport sur la proposition de règlement*, Jan Philipp Albrecht, Doc. A7-0402-2013 du 21 nov. 2013

- Conseil d'Etat, rapport annuel 2014 : *le numérique et les droits fondamentaux,* doc. Fr., 2014

- Avis du contrôleur européen de la protection des données, *relever les défis des données massives : un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes*, JO C 67, 20 fév. 2016. 13-15

- Guidelines on the right to data portability, adopted on 13 december 2016, Article 29 Data protection working party (G29, WP 242)

- Avis n°01/2017 du 4 avril 2017 sur la proposition de règlement « vie privée et communications électroniques », Groupe de travail « Article 29 » sur la protection des données (G29, WP 247)

SITES INTERNET :

- Commission Nationale de l'Informatique et des Libertés, *Ethique et numérique : les algorithmes en débat,* [en ligne] 23 janv. 2017
Disponible sur : <https://www.cnil.fr/fr/ethique-et-numerique-les-algorithmes-en-debat>

- LAUSSON, J., *167 millions d'accès Linkedln piratés : le vôtre aussi ?* , [en ligne] Numerama, 24 mai 2016
Disponible sur http://www.numerama.com/tech/172291-167-millions-dacces-linkedin-pirates-le-votre-aussi.html

- LEFEBVRE, J.-S., *Déjà 20 mois de négociations sur les données personnelles,* [en ligne] Contexte Numérique, 9 sept. 2015
Disponible sur : < https://www.contexte.com/article/numerique/donnees-personnelles-lobbying-americain-massif-a-bruxelles_20211.html >

- Le Monde, *500 millions de comptes, d'utilisateurs Yahoo ! ont été piratés,* [en ligne] Chronique (r)évolution, 22 sept. 2016
Disponible sur : <http://www.lemonde.fr/pixels/article/2016/09/22/500-millions-de-comptes-d-utilisateurs-de-yahoo-ont-ete-pirates_5002118_4408996.html>

- SCHWAB P.-N., *RGPD : qu'est-ce que le concept de portabilité des données ?* [en ligne] Into the minds, 14 juin 2017
Disponible sur : < http://www.intotheminds.com/blog/?s=portabilit%C3%A9>

DECISIONS ET RAPPORTS DE LA CNIL :

- Délibération n°2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux cookies et autres traceurs visés à l'article 32-II de la loi du 6 janvier 1978
- Délibération de la formation restreinte n°2013-420 du 3 janvier 2014 prononçant une sanction pécuniaire à l'encontre de la société X
- Délibération de la formation restreinte n°2015-155 du 01 juin 2015 prononçant une sanction pécuniaire à l'encontre de la société PRISMA MEDIA
- Délibération n°2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et prospects

- Délibération de la formation restreinte n°2016-265 du 20 septembre 2016 prononçant un avertissement public à l'encontre de la société CDISCOUNT
- Rapport d'activités 2016
- Conférence de presse du 27 mars 2017, *rapport d'activités 2016 et des enjeux 2017*

TABLE DES MATIERES

Remerciements …… p. 1

Sommaire ……..…… p. 2

Liste des principales abréviations ……. p. 3

Introduction ……..…… p. 4

PREMIERE PARTIE

LE RENFORCEMENT DES OBLIGATIONS DE L'E-COMMERCANT

Chapitre I – La mise en place d'une stratégie de gouvernance des données …… p. 9

Section I – Le respect du principe d'accountability …… p. 9

§1 – La consécration du principe …… p. 9

A. Un principe d'origine anglo-saxonne ……. p. 10

B. L'expansion du principe dans l'Union européenne …….. p. 11

§2 – Un changement de paradigme eu égard à la règlementation actuelle …….. p. 12

A. La fin des formalités préalables …….. p. 12

B. L'adoption de mesures internes contraignantes …… p. 14

Section II – Le respect du principe de privacy by design …….. p. 15

§1 – La consécration d'un principe de responsabilisation …… p. 16

A. La genèse du principe …….. p. 16

1. Au Canada ……... p. 16

2. En Europe …… p. 17

B. Une nouveauté en droit français ……. p. 17

§2 – La mise en œuvre du principe …….. p. 20

A. L'adoption de mesures techniques efficaces …….. p. 20

B. La difficile implémentation du principe …… p. 22

Chapitre II – L'analyse des risques du traitement sur la vie privée ……. p. 24

Section I – L'encadrement du recours au profilage ……... p. 24

§1 – Une pratique classique d'e-commerce …… p. 25

A. La proposition de contenu personnalisé …… p. 25

1. La définition du profilage …….. p. 25

2. Les techniques de profilage …… p. 27

B. Les risques engendrés par la pratique ……... p. 27
§2 – Une pratique au recours conditionné ……. p. 28
A. La licéité du traitement aux fins de profilage …… p. 28
1. L'intérêt légitime de l'e-commerçant …….. p. 29
2. La détermination des finalités du profilage …….. p. 30
B. L'information des consommateurs sur la logique du profilage …… p. 30
1. L'obligation d'information sur la logique du profilage …… p. 31
2. Vers un contrôle plus accru du profilage ……. p. 31
Section II – La notification des violations de données ……... p. 33
§1 – Une coopération avec l'autorité de contrôle ……... p. 34
A. Une coopération textuelle efficace …….. p. 34
B. Une coopération complexe en pratique …….. p. 36
1. La détermination d'un risque pour les droits et les libertés des personnes physiques …….. p. 36
2. Le délai de notification de 72 heures ……... p. 37
§2 – Une communication à la personne concernée …… p. 38

DEUXIEME PARTIE

LE RENFORCEMENT DES DROITS DES CONSOMMATEURS

Chapitre I – Le renforcement des droits préalablement à la collecte …… p. 42
Section I – Une information transparente ……. p. 43
§1 – L'exhaustivité de l'information ……... p. 44
A. L'information en cas de collecte auprès de la personne concernée …….. p. 44
B. L'information en cas de collecte auprès d'une tierce personne …… p. 46
§2 – L'accessibilité de l'information ……... p. 46
A. La teneur du droit à une information accessible ……... p. 47
B. La contradiction d'une information transparente …… p. 48
Section II – Un consentement éclairé sur la base de l'information …… p. 49
§1 – La consistance du renforcement du consentement ……... p. 49
A. Une notion unifiée à l'échelle européenne …….. p. 50
1. Une notion antérieure sujette aux divergences nationales …… p. 50
2.La notion de consentement au sens du Règlement ……. p. 51

B. La gestion clarifiée du consentement ……. p. 51
1. La manifestation du consentement …….. p. 51
2. Le retrait du consentement ……... p. 53
§2 – Les craintes sur la place laissée au consentement …….. p. 54
A. La légitimité du consentement …… p. 54
B. Le fondement de l'intérêt légitime du responsable du traitement ……... p. 55
Chapitre II – Le renforcement des droits postérieurement à la collecte …….. p. 57
Section I – La mise en œuvre d'un droit à la portabilité des données ……... p. 57
§1 – La consécration d'un droit à la portabilité ……. p. 58
A. De la portabilité des services ……... p. 58
B. A la portabilité des données …… p. 59
1. L'introduction du concept dans le règlement …….. p. 59
2. L'anticipation du concept en droit interne …….. p. 60
§2 – Les modalités d'exercice du droit à la portabilité …….. p. 62
A. La faisabilité du transfert ……... p. 62
B. La limitation des données portées …….. p. 63
1. Des données relatives au titulaire du droit ……... p. 63
2. Des données fournies par le titulaire du droit …….. p. 64
Section II – La portée du droit à la portabilité …… p. 65
§1 – Une maitrise sur le traitement opéré …….. p. 65
§2 – Une maitrise nuancée ……... p. 67
A. Un droit d'accès limité ……. p. 67
B. Un droit consumériste ……. p. 69

Conclusion ……... p. 70
Bibliographie …… p. 72
Table des matières ……... p. 79