Le droit d'accès aux données à caractère personnel : réflexions sur un éventuel rapprochement du droit continental et anglo-saxon

Angela Cubillos Vélez*

16 febbraio 2017

SOMMAIRE : 1. Introduction – 2. Le rapprochement récent des systèmes juridiques - 2.1. Le recul de la protection des données personnelles dans le système juridique européen – 2.2. Le renforcement de la protection des données personnelles dans le système anglo-saxon – 3. Une disparité de régimes pourtant existante - 3.1. Les vides juridiques du système américain – 3.2. Le maintien du renforcement de la protection des données dans le système continental.

1. Introduction

L'une des pierres angulaires du gouvernement ouvert est le principe du libre accès du public aux documents administratifs. Les deux grands systèmes juridiques (continental et anglo-saxon) ont reconnu ce droit aux citoyens[1]. Cette liberté s'étend à tous les documents et toutes les informations détenues par l'administration publique. Cependant, ce droit d'accès connaît des limites qui sont sensiblement les mêmes mais à des degrés différents d'un système juridique à l'autre. Nous avons ainsi trois types d'information et trois modalités d'accès différentes :

INFORMATION	MODALITÉ D'ACCÈS
INFORMATION PUBLIQUE LIBRE. DONNÉES OUVERTES	Information en libre accès sur Internet sans demande préalable nécessaire. La réutilisation de l'information est permise.
INFORMATION PUBLIQUE RÉSERVÉE. Données concernant la défense ou la sécurité nationale, la sécurité publique, les relations internationales, ou relatives à un délit commis, etc.	Information ne pouvant en aucun cas être mise en accès libre dans la mesure où cela peut nuire à l'intérêt public. Le refus doit être motivé et signifié par écrit.

* Avocate, professeur-chercheur à l'Université Externado de Colombie, membre fondatrice du Centre de Recherche de Droit Informatique CIDI. Doctorante Université Paris 1 Panthéon-Sorbonne.

[1] http://www.cada.fr/la-liberte-d-acces-en-europe-et-dans-le-monde,6084.html **«** La législation la plus ancienne est celle de la Suède, qui reconnaît le droit d'accès depuis 1776, droit réaffirmé par la loi constitutionnelle de 1974. Les législations des autres pays sont beaucoup plus récentes : le **« Freedom of Information Act » (FOIA) aux États-Unis date de 1966** ; la constitution espagnole reconnaît le droit à l'information depuis 1978 ; l'Italie depuis la loi du 7 août 1990 ; en Grande-Bretagne les deux lois qui concernent le droit d'accès sont entrées en vigueur en 2005 ; et en Allemagne la loi fédérale sur le sujet est entrée en vigueur en 2006 ». Au niveau européen Directive 2003/98/CE et Directive/37/UE.

INFORMATION APPARTENANT A LA SPHERE PRIVEE D'UNE PERSONNE.	Données susceptibles d'être restreintes sauf si la personne morale ou physique autorise la publication. Une demande préalable est requise. Il faut justifier d'un intérêt particulier pour obtenir l'accès aux documents. La réutilisation est exclue ou limitée pour les documents contenant des données à caractère personnel. Elle est également limitée pour les documents accessibles qui contiennent en partie des données à caractère personnel. Car la réutilisation devient incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel. La demande d'information peut être également refusée lorsqu'il y a un risque portant sur la vie, la santé, la vie privée, ou la sécurité d'une personne.

Dans cet article, nous nous concentrerons sur le droit d'accès aux données à caractère personnel en faisant une analyse en droit comparé européen et américain, afin d'examiner si un rapprochement des systèmes a lieu actuellement, entre autres, avec l'adoption du règlement général relatif à la protection des données personnelles. Un examen des systèmes juridiques permettra d'établir ainsi les points communs concernant la protection de la vie privée. Cette analyse est nécessaire car l'écart entre les régimes entrave la protection des données dans l'ère du numérique, d'où la réconciliation entre les deux régimes s'avère nécessaire.

Or, concernant la protection de la vie privée, une problématique se pose lorsque le traitement de données est notamment réalisé en dehors d'un territoire qui assure un niveau de protection supérieur à celui du territoire de destination. Etant donné que ce qui pourra être considéré comme ayant un caractère de donnée privée dans le système Européen, pourra être considéré comme ayant un caractère de donnée publique dans le système anglo-saxon, où l'importance d'identifier les proximités et les disparités des régimes.

Sur ce point, il est important de noter que deux acceptions sur la protection de données persistent encore de nos jours dans le monde : la première englobe un sens personnaliste dans sa définition, considérant que les données personnelles sont un attribut de la personnalité. Cette position est présente dans le modèle européen actuel. La deuxième considère que les données personnelles sont des biens pouvant être vendus. Cette doctrine, qui favorise la croissance économique, trouve sa place dans le système américain, ce système n'est pas considéré en Europe comme assurant un niveau de protection adéquat.

Malgré cette disparité de régimes, il est possible de se poser la question de savoir s'il existe actuellement un rapprochement de régimes ? pour répondre à cette question on examinera tout d'abord si ces systèmes juridiques se sont rapprochés récemment, puis on présentera la disparité de systèmes qui est désormais présente.

2. Le rapprochement récent des systèmes juridiques

On assiste à un double phénomène : tout d'abord, au recul du modèle de protection des données personnelles dans le système européen, puis au renforcement de cette protection dans le système anglo-saxon.

2.1. Le recul de la protection des données personnelles dans le système juridique européen

Pour examiner ce phénomène juridique, il est important de préciser qu'au niveau européen, la Directive de 1995 assurait une protection qui a été récemment reformée par le règlement général sur la protection des données personnelles de 2016 qui entrera en vigueur en 2018. En faisant une comparaison des régimes, il est possible d'observer les modifications suivantes :

La Directive 1995	**Réglement général de protection des données de 2016**
Objet de la directive 1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, **notamment de leur vie privée,** à l'égard du traitement des données à caractère personnel[2].	**Objet et objectifs** **Il n'y a pas de référence à la protection de la vie privée.** 1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données[3].
Définition des données à caractère personnel et de personne concernée Toute information **concernant** une personne physique identifiée ou identifiable[4].	**Définition des données à caractère personnel et de personne concernée** Le règlement augmente la maîtrise par chacun de ses données. Article 4 Règlement 2016. « données à caractère personnel», toute information se **rapportant** à une personne physique identifiée

[2] Article 1. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[3] Article 1. 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.
[4] Article 2. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. « Données à caractère personnel : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ».

	ou identifiable (ci-après dénommée «personne concernée») ».
Désignation de l'Autorité de contrôle dans l'UE Compétence territorial lieu de l'Etat membre du lieu du traitement des données.	**Désignation de l'Autorité de contrôle dans l'UE** Désignation de l'Autorité de contrôle du lieu d'établissement principal d'un groupe d'entreprises opérant sur le territoire européen. **Critique :** « C'est une simplification non négligeable pour les groupes opérant dans plusieurs états membres »[5]. La notion même d'établissement principal est ambiguë[6]. « Une forme de forum shoping risque de se mettre en place puisque les entreprises pourront soumettre leur traitement à l'autorité de contrôle la plus (clémente) »[7].
Contrôle Logique du système de contrôle exercé en amont par l'autorité de contrôle.	**Contrôle** On assiste à une simplification des contrôles. Ici il est possible de s'intéresser sur la légitimité. Sur la simplification des contrôles deux réflexions sortent de la lecture du Règlement :

[5] MARTIAL-BRAZ, Natalie. *La proposition de règlement européen relatif aux données à caractère personnelle : propositions du réseau Trans Europe Experts.* Société de législation comparée. Paris. 2014. p. 179.

[6] Article 4. 16. 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. **Etablissement principal** « a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal.

b) en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement ».

[7] MARTIAL-BRAZ, Natalie. *cit.*, p. 179.

	Premièrement, on assiste à une simplification des contrôles en réduisant les formalités préalables. La logique du nouveau Règlement est la suppression des formalités préalables auprès des autorités de contrôle (la CNIL en France). Sauf exception, il n'y a donc plus de déclaration ou de demandes d'autorisation préalable à la mise en place de traitements de données à caractère personnel. Ce système est substitué par un contrôle *a posteriori* « fondé sur les actions coercitives de l'autorité de contrôle"[8]. **Problème :** le Règlement enlève le système de prévention, la sanction intervient quand la menace à la protection de la vie privée est déjà parvenue, comme dans le système américain où il n'existe pas de contrôle préalable du traitement des données.
Contrôle externe Seulement l'autorité de contrôle examine la mise en conformité.	**Contrôle interne** Deuxièmement, il existe une **responsabilisation des entreprises** sur la question du traitement des données personnelles. Notamment avec l'obligation pour certaines entreprises de désigner un délégué à la protection des données[9]. Certaines entreprises doivent instaurer un système d'audit interne avec la désignation du délégué à la protection des données.
Pouvoir d'investigation	**Pouvoir d'investigation** Limitation du pouvoir d'investigation de l'autorité de contrôle.

[8] MARTIAL-BRAZ, Natalie. *cit.*, p. 303.

[9] Article 37. 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. « Désignation du délégué à la protection des données.

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».

Pouvoir effectif d'intervention sans qu'une demande d'autorisation judiciaire préalable soit requise. Pouvoir d'agir de manière autonome sans contrôle judiciaire pour l'exercice du pouvoir d'investigation[10].	La constatation des éventuelles manquements à la loi est conditionnée à l'existence d'une autorisation judiciaire préalable. Une saisine du juge devient obligatoire[11]. Cela met en risque la stratégie de contrôle mise en œuvre par l'autorité de contrôle pour constater d'éventuels manquements à la loi sans motif raisonnable de supposer l'existence d'une activité contraire aux dispositions.
Directive de 95 applique uniquement le droit dur.	**Création des codes de conduite** Ici on assiste à une contractualisation des relations entre responsable de traitement et personne concernée. La réglementation « crée toutes les conditions pour que les codes de conduite privés puissent constituer une matière véritablement essentielle du droit vivant de la protection des données. Ce qui pose la question du contrôle de ces normes privées »[12].

2.2. Le renforcement de la protection des données personnelles dans le système anglo-saxon

Le droit d'accès à l'information connaît également des limites en droit américain. L'amendement de 2007 du *freedom of information act* limite l'accès aux données qui peuvent représenter une atteinte injustifiée à la vie privée[13]. Dans le même sens, *the Federal Information Security Modernization Act* de

[10] Article 28. 3. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. « Chaque autorité de contrôle dispose notamment :
- de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,
- de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques ».

[11] Article 58. f. 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. "obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres ».

[12] MARTIAL-BRAZ, Natalie. *cit.*, p. 346.

[13] https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/amended-foia-redlined.pdf. The Freedom of Information Act, 5 U.S.C. § 552 As Amended By Public Law No. 110-175, 121 Stat. 2524. « (b) This section does not apply to matters that are : (…)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (…) (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy ».

2014 donne une définition de la sécurité de l'information et de confidentialité. Elle consacre notamment des restrictions au sujet de l'accès, la divulgation, la protection et la confidentialité de la vie privée[14].

Concernant la protection des données personnelles, le droit américain est dépourvu d'une loi générale, cependant, il existe déjà une panoplie de **lois fédérales sectorielles** relatives à la protection de la vie privée régissant la collecte et l'utilisation de données personnelles. Voici quelques-unes des lois fédérales les plus importantes en matière de protection des données personnelles :

- La Federal Trade Commission Act (15 U.S.C. §41-58) (FTC Act) est une loi fédérale sur la protection du consommateur qui interdit les pratiques déloyales ou trompeuses et qui s'applique aux politiques de confidentialité en ligne.

- Loi sur la lutte contre l'assaut de pornographie et de marketing non sollicités (Loi CAN-SPAM) (15 USC §§7701-7713 et 18 USC §1037) et la *Telephone Consumer Protection Act* (47 USC §227 et suivants) Traitent la collecte et l'utilisation des adresses e-mail et des numéros de téléphone, respectivement.

- En 2016, le Congrès a promulgué la Loi sur la réparation judiciaire, qui donne aux citoyens de certains pays alliés (notamment les États membres de l'UE) le droit de demander réparation aux tribunaux américains pour violation de la vie privée.

Les Etats-Unis disposent également d'une centaine de **lois sur la protection des renseignements personnels et de la sécurité des données parmi ses 50 États** et territoires (y compris plus de 25 lois sur la protection de la vie privée et la sécurité des données dans le seul État de Californie).

Les lois les plus représentatives proviennent de l'Etat de Californie : *the California Security Breach Notification Law,* qui s'applique à toute personne ou entreprise qui exerce ses activités en Californie et qui possède ou autorise des données informatisées comprenant des données personnelles. Et *the California Online Privacy Protection Act,* qui s'applique à l'exploitant d'un site Web commercial, d'un service en ligne ou d'une application mobile qui collecte des informations personnelles identifiables par Internet sur les consommateurs résidant en Californie qui utilisent ou visitent son site Web commercial ou son service en ligne. Avec la présentation de ce cadre juridique américain, il est possible d'affirmer qu'on assiste à un renforcement de la protection des données personnelles.

En outre, concernant l'organisme de réglementation ou autorité nationale chargée de la protection des données, il n'existe pas d'autorité nationale officielle de protection des données. Cependant, la Federal Trade Commission FTC a la compétence sur la plupart des entités commerciales et elle détient le pouvoir d'émettre et d'appliquer des règlements sur la protection des données personnels

---

[14] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf Federal Information Security Modernization Act of 2014. 44 USC 101 note. Public Law 113–283 113th Congress An Act To amend chapter 35 of title 44, United States Code, to provide for reform to Federal information security. PUBLIC LAW 113–283—DEC. 18, 2014 "§ 3552. Définitions « (3) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide. (B) 'confidentiality', which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information ».

dans des domaines spécifiques, p. Ex. Loi sur la protection de la vie privée des enfants en ligne ou Children Online Privacy Protection Act.

La Federal Trade Commission (FTC) applique également des instruments juridiques contre les entreprises qui ne mettent pas en œuvre des mesures adéquates de protection des données et des politiques de confidentialité. Elle autorise également les politiques de traitement ou de divulgation de données personnelles.

Concernant la collecte et le traitement des données, les lois et règlements américains sur la protection de la vie privée varient considérablement mais contiennent généralement l'obligation d'informer sur la collecte, l'utilisation et la divulgation des informations personnelles. En outre, s'agissant des exigences en matière de notification, the California Online Privacy Protection Act requiert des sites Web du e-commerce la divulgation de leurs pratiques en matière de protection de la vie privée.

Dans le même sens, concernant la publicité ciblée, la FTC suggère aux opérateurs de sites Web informer sur leurs pratiques de collecte de données liées à la publicité ciblée en ligne, en fournissant aux consommateurs les mécanismes d'exclusion de ce type de publicité. Les États-Unis réglementent également strictement les communications de marketing, y compris le courrier électronique et le marketing de messages texte, ainsi que le marketing par télémarketing et par télécopieur.

S'agissant des données personnelles sensibles, elles comprennent les données financières, les données sur les enfants strictement protégées par le COPPA (Children Online Privacy Protection Act)[15], les informations sur la santé, les informations précises sur l'emplacement géographique et les numéros de sécurité sociale.

S'agissant des sanctions, des amendes substantielles sont généralement imposées par le FTC. Le FTC Act prévoit des pénalités allant jusqu'à 16 000 $ US pour chaque infraction. Le FTC peut également chercher à obtenir une injonction, une indemnisation des consommateurs et le remboursement des frais d'enquête et de poursuite. Du surcroît, les peines criminelles comprennent l'emprisonnement pouvant aller jusqu'à dix ans.

Malgré la reconnaissance partielle de la protection des données aux Etats Unis, il demeure nécessaire que les sociétés prestataires de services d'internet américaines ne doivent pas s'en contenter et doivent réfléchir à la mise en place et à l'application de leurs propres standards dans le domaine du respect de la vie privée des internautes. Les Etats-Unis ont répondu à la croissance exponentielle du commerce électronique par un patchwork de mesures ponctuelles et de lois. Cependant cela n'assure pas une protection générale des données des personnes concernées.

3. Une disparité de régimes pourtant existante

3.1. Les vides juridiques du système américain

15 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule Children's Online Privacy Protection Rule ("COPPA"). Text of rule and final rule amendments.

L'un des éléments clé pour affirmer qu'il existe un rapprochement des régimes est la définition des données personnelles, qui est indispensable afin de fixer l'étendue de la protection et d'établir son champ d'application. Cependant, elle est absente en droit américain. On constate qu'il n'y a pas un rapprochement des concepts entre les deux régimes juridiques, ainsi, la protection est difficile, notamment car ce qui est considéré comme une donnée à caractère personnel en Europe, n'est pas nécessairement considéré comme ayant un caractère privé aux Etats Unis. Il en ressort qu'une donnée considérée comme personnel en Europe puisse être dépourvue de protection dans le système juridique américain.

Plusieurs vides juridiques non négligeables persistent dans le système américain :

Concernant la loi sectorielle américaine, *Federal Trade Commission Act*, il est important de noter que malgré l'existence d'une protection du consommateur grâce aux politiques de confidentialité, cette loi n'exige pas expressément qu'une entreprise divulgue sa politique de confidentialité.

Cependant, si une entreprise divulgue une politique de confidentialité, elle doit s'y conformer. De plus, la FTC a déclaré que le fait pour une société de modifier sa politique de confidentialité sans fournir cette information et demander l'autorisation aux personnes concernées, constitue une violation du Federal Trade Commission Act.

S'agissant du consentement, qui est l'un des points importants de toute réglementation concernant la protection des données personnelles, la FTC considère que les opérateurs de sites Web doivent obtenir un consentement explicite avant d'utiliser les données sensibles des consommateurs. Néanmoins, le FTC Act and the California Online Privacy Protection Act ne traitent pas spécifiquement la question relative aux exigences générales du consentement, ce qui ne permet pas d'assurer une protection suffisamment encadrée et qui laisse la porte ouverte à des actes discrétionnaires de la part du responsable du traitement.

Au sujet du droit à l'oubli, les personnes concernées n'ont actuellement pas le droit de demander la suppression de leurs données en vertu des lois fédérales applicables. Du surcroît, une partie de la doctrine américaine considère que la reconnaissance de ce droit entraîne une violation du premier amendement de la Constitution américaine, qui protège par ailleurs les libertés d'information et d'expression.

À propos de la déclaration ou de l'enregistrement des traitements auprès de l'autorité chargée, il n'est pas nécessaire d'enregistrer des bases de données contenant des données personnelles, selon les dispositions américaines en vigueur. Dans le même sens, il n'est pas réquis non plus de nommer un responsable de la protection des données. Cependant, nommer un privacy officer et un IT security officer est devenue une pratique exemplaire.

L'utilisation des données à caractère personnel par les grandes entreprises américaines d'Internet est également très variée et difficile à contrôler aujourd'hui. Il existe aujourd'hui une monétisation des données personnelles de l'audience, par exemple grâce au modèle biface de gratuité. Ainsi, l'on constate la création de publicité ciblée, l'installation de cookies, la surveillance, la localisation et l'identification des personnes concernées grâce à l'application du Big Data.

3.2. Le maintien du renforcement de la protection des données dans le système continental

Malgré l'existence d'un recul sur certains aspects de la protection des données à caractère personnel, il est possible d'observer que la tendance du système continental et notamment du droit européen est de maintenir et d'assurer la protection des données. Il est constatable que, la conception personnaliste des données a été introduite au début du règlement dans les considérants 1 et 2.

En outre ce renforcement est présent tout au long du Règlement. Par comparaison entre la Directive de 95 et le Règlement de 2016, on peut noter les améliorations suivantes :

1. Tout d'abord le Règlement défini des notions essentielles non contenues dans l'ancienne Directive de 1995. Elle précise ce qu'il faut comprendre par « limitation du traitement» ; par «profilage» ; par «pseudonymisation» ; par « violation de données à caractère personnel » ; « données génétiques » ; « données biométriques » ; « données concernant la santé » par «établissement principal» ; «représentant» ; «règles d'entreprise contraignantes»[16].

2. Puis, le Règlement reconnait comme principe la sécurité des données[17] qui n'était pas prévue dans la Directive de 95, ainsi, l'obligation de protection contre les traitements non autorisés ou illicites et contre le risque de perte d'intégrité ou de confidentialité est actuellement une garantie exigible qui occupe un rang supérieur.

3. Un renforcement important du pouvoir de sanction des autorités de contrôle a été prévu. Car sur la Directive de 1995 les sanctions restaient symboliques notamment s'agissant des grandes entreprises prestataires des services d'internet[18].

4. Il existe également un renforcement de l'obligation d'information aux personnes concernées, l'obligation de recueillir leur consentement préalable avant la collecte des données a été également renforcée. Les responsables du traitement doivent être en mesure de prouver que le consentement a été donné, ce consentement doit être donnée par une déclaration ou une action affirmative et claire.

5. L'encadrement du contrat de sous-traitance, devra contenir des dispositions impératives pour limiter le pouvoir de traiter les données sur les instructions explicitement contenues. De même, l'obligation d'assurer la sécurité des données est désormais présente, notamment en cas de transferts des données hors Union Européenne.

---

[16] Article 4. 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.

[17] Article 5. 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.

[18] Article 83. 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. Conditions générales pour imposer des amendes administratives. « 4. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent (…)
5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent (…)
6. Le non-respect d'une injonction émise par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, fait l'objet, conformément au paragraphe 2 du présent article, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ».

6. En matière des données détenues par l'administration, la désignation du délégué à la protection des données se rend obligatoire[19], il peut être un membre du personnel de l'entité ou un prestataire externe.

On peut conclure ainsi que, le Règlement de 2016 renforce d'avantage la protection existant au niveau européen, on n'assiste donc pas seulement au maintien mais à l'élargissement de cette protection des données personnelles. Ce qui entraîne sur certains points un écart plus prononcé entre les deux systèmes juridiques analysés.

Trois remarques complémentaires peuvent être apportées : premièrement, les différences entre les États-Unis et l'Union européenne en matière de protection de données personnelles sont multiples[20] et ces antagonismes empêchent l'unification des systèmes. Deuxièmement, les différences son conciliables, en matière de transfert international des données, plusieurs outils (clauses contractuelles, régles d'entreprise contraignantes, etc) ont été créés afin de transférer des données à caractère personnel depuis les pays européens vers les Etats Unis[21]. L'annulation des accords *safe harbor* et la récente adoption du *Privacy Shield* vise également à renforcer cette protection, les sociétés américaines effectuant des traitements des données en Europe doivent d'abord adhérer au système de *Privacy Shield*, cela permet de veiller au respect des engagements des entreprises, notamment, car elles sont soumises à l'obligation du respect des principes de protection de la vie privée ou *Privacy Principles*.

Troisièmement, sur le rapprochement des systèmes juridiques, une dichotomie reste présente entre le droit du consommateur et la liberté fondamentale. En effet, en Europe, les données personnelles appartiennent au champ des libertés fondamentales et on considère qu'elles font partie des attributs de la personnalité[22]. À l'inverse, aux Etats-Unis, la protection des données est davantage traitée sous le prisme de la protection du consommateur et il existe une vision patrimoniale des données.

Finalement, en ce qui concerne le droit d'accès aux documents publics, ce droit devrait garantir l'une de ces trois fonctions essentielles :

1 - assurer la participation démocratique et l'exercice des droits politiques ;
2 - permettre la matérialisation d'autres droits constitutionnellement reconnus ;
3 - garantir la transparence de la gestion publique et le contrôle de l'activité de l'Etat effectué par les citoyens.

En dehors de ses finalités, une utilisation des données à des fins différentes risque de dénaturer l'exercice du droit, d'où l'importance d'assurer une protection de la vie privée des citoyens, par exemple : la monétisation de l'information ne constitue pas une finalité légitime à l'origine du droit à l'accès à l'information publique. La réutilisation des données effectuée à des fins de surveillance et de monétisation des données personnelles est également contraire aux finalités légitimes, même si elle est effectuée par l'Etat.

---

[19] Il est le nouveau Correspondant Informatique et Libertés (CIL).

[20] UE et États-Unis peinent à concilier leurs approches de protection des données. (En ligne) http://www.euractiv.fr/section/societe-de-l-information/news/ue-et-etats-unis-peinent-a-concilier-leurs-approches-de-protection-des-donnees/ 11 janv. 2016 (mis à jour: 30 mars 2016).

[21] http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_fr.pdf Guide du bouclier de protection des données UE-Etats-Unis. Guide de privacy shield édité par la Commission Européenne.

[22] Article 8 de la Charte des droits fondamentaux de l'Union européenne, qui prévoit le «droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance».

Ainsi, un contrôle de l'utilisation ultérieure des données personnelles détenues par l'administration publique s'avère indispensable. La réutilisation des données « Implique aussi que leur qualité et leur intégralité soient garanties et que les jeux de données réutilisables comportent des éléments de contextualisation et de description (méta-données) permettant leur intelligibilité »[23]. La dénaturation des informations publiques devrait faire l'objet de sanction, sauf si elle est autorisée par l'administration dans le respect de la réglementation en vigueur.

La réutilisation de l'information publique comportant des données personnelles doit respecter la réglementation en vigueur. Ainsi, l'on ne peut pas se prévaloir du droit d'accès à l'information publique pour réutiliser l'information à des finalités contraires aux principes consacrés dans la règlementation sur la protection des données à caractère personnel en Europe, d'où l'importance d'harmoniser les systèmes juridiques. Il est important de promouvoir cette liberté au droit d'accès, tout en protégeant la vie privée des individus, notamment s'agissant de transfert des données vers de pays tiers assurant un niveau inférieur de protection. L'intérêt doit être concentré non seulement sur la finalité de la réutilisation, mais également sur le type d'information réutilisé. La personne concernée doit donner son accord si la finalité du traitement ultérieur est différente[24].

[23] P. CANACAGGIO. *Vers un droit d'accès à l'information publique*. Les avances récentes des normes et des pratiques, UNESCO, 2014.

[24] Groupement Français de l'Industrie de l'Information Synthèse du séminaire organisé par le groupe de travail « Diffusion des données publiques ». 19 novembre 2004. Assemblée Nationale. Consulté le 10 janvier 2016. [http://www.gfii.fr/uploads/docs/la-reutilisation-des-donnees-publiques-un-enjeu-majeur-pour-la-societe-europeenne-de-l-information.pdf].