FABRISSIN Pierre-Yves

Master 2 Droit de l'entreprise - Spécialité Droit de l'Immatériel et des Technologies de l'Information - Parcours Propriété Intellectuelle.

Année universitaire 2015/2016

SUJET DU MEMOIRE

La protection européenne des données personnelles : actualité et perspectives.

DIRECTEUR DU MEMOIRE : Madame le Professeur Alexandra Mendoza-Caminade

L’université n’entend donner aucune approbation ni improbation aux opinions émises dans les mémoires ; ces opinions devront être considérées comme propres à leurs auteurs.

« Tout ce que vous direz pourra et sera utilisé contre vous ».

Tout bon policier américain procédant à une arrestation.

Extrait des « Droits Miranda » dégagés par la Cour Suprême des États-Unis le 13 juin 1966 dans l'affaire « MIRANDA v. ARIZONA ».

Liste des principales abréviations utilisées

CA : Cour d'appel.

CEDH : Convention/Cour européenne des droits de l'homme.

CEPD : Comité européen de la protection des données.

CGU : conditions générales d'utilisation.

CGV : conditions générales de vente.

CIL : Correspondant « informatique et libertés »

CJCE : Cour de justice des communautés européennes.

CJUE : Cour de justice de l'Union européenne.

CNIL : Commission nationale de l'informatique et des libertés

DPO : « Data Protection Officer »

EDPS : « European Data Protection Supervisor »

FAI : fournisseur d'accès Internet.

G-29 : Groupe de travail « article 29 »

LCEN : Loi pour la confiance en l'économique numérique.

NIR : Numéro d'inscription au répertoire ou « numéro de sécurité de sociale ».

PIA « Privacy impact assessment » ou analyse des risques.

RGPD : Règlement général de la protection des données.

TFUE : Traité sur le fonctionnement de l'Union européenne.

Sommaire

INTRODUCTION **9**

PARTIE 1 - HARMONISATION DE LA PROTECTION DES DONNEES PERSONNELLES DANS L'UE. **27**

CHAPITRE 1 : LES CONTOURS D'UNE « DECLARATION DES DROITS DE L'HOMME » A L'ERE DU NUMERIQUE. 29

I. La réaffirmation et l'évolution des principes relatifs à la protection de la personne. *31*

II. L'extension de la régulation des pratiques du responsable de traitement. *41*

CHAPITRE 2 : LA COLLABORATION DES INSTITUTIONS DE REGULATION A LA PROTECTION DES DONNEES PERSONNELLES. 58

I. L'intervention de la Commission nationale de l'informatique et des libertés. *59*

II. Les autres autorités intervenant dans le processus de régulation. *70*

PARTIE 2 – L'INTEGRATION DES DONNEES PERSONNELLES DANS LE MARCHE ECONOMIQUE NUMERIQUE. **76**

CHAPITRE 1 : L'ACCROISSEMENT DES DEBOUCHES COMMERCIAUX POUR LES DONNEES PERSONNELLES : L'INTEGRATION DANS LE « MARCHE UNIQUE NUMERIQUE ». 78

I. Promouvoir la circulation des données personnelles en restaurant la confiance des citoyens européens. *81*

II. Promouvoir la circulation des données personnelles tout en responsabilisant les opérateurs du numérique. *89*

CHAPITRE 2 : LA REGULATION DU TRANSFERT DE DONNEES PERSONNELLES EN DEHORS DE L'UNION EUROPEENNE. 99

I. Le « droit commun » de l'exportation des données personnelles : la recherche d'une protection territoriale « adéquate ». *101*

II. La diplomatie dans l'exportation des données personnelles : l'édification d'une adéquation sectorielle. *108*

CONCLUSION **115**

Introduction

« Nous parlons d'un enjeu qui concerne chacun d'entre nous, de notre capacité de travail, à la maison, dans nos achats, notre santé, à voir notre vie privée effectivement garantie au sein d'un univers qui a tellement changé depuis dix ans. En quelques années en effet, le monde numérique s'est installé. Il ne s'agit pas seulement d'Internet. Il s'agit de la dématérialisation progressive de toutes les activités humaines qui s'étendent désormais du monde physique au monde virtuel ; l'individu passe de l'un à l'autre souvent sans même s'en apercevoir et la donnée est au cœur de ce monde sans couture ».[1]

Isabelle Falque-Pierrotin

Présidente de la CNIL[2]

Pour commencer, il nous faut indiquer que le présent mémoire de recherches n'a pas la prétention d'envisager la totalité des évolutions européennes dans le droit de la protection des données personnelles mais d'initier une réflexion autour de cette problématique. Il s'agira d'en dégager les enjeux ainsi que les mécanismes principaux mis en œuvre par les institutions européennes, qui cherchent à concilier le développement de l'économie numérique, d'un côté, et l'Etat de droit et la protection des libertés fondamentales des citoyens européens, de l'autre. Notre réflexion se limitera alors à l'aspect économique des données personnelles et ne s'étendra pas aux considérables impacts démocratiques que leur traitement peut représenter.

La notion même de « donnée » peut présenter différentes acceptions. Selon le dictionnaire Larousse, la donnée est la « *représentation conventionnelle d'une information en vue de son traitement informatique* ». Elle peut également prendre le sens de « *résultats d'observations ou d'expériences faites délibérément ou à l'occasion d'autres tâches et soumis aux méthodes statistiques* ». L'appréhension de la donnée est alors davantage fonction de l'usage qui en est fait que de sa nature propre. Il s'agit d'une information, quelle qu'elle soit et peu important la forme sous laquelle elle se présente, qui a vocation à subir un traitement informatique ou statistique.

---

[1] *Isabelle Falque-Pierrotin, « Quelle protection européenne pour les données personnelles ? », Fondation Robert Schuman, Questions d'Europe, n° 250, 3 septembre 2012.*

[2] *Commission Nationale de l'informatique et des libertés (CNIL)*

Selon le Conseil économique, social et environnemental, le sens commun attaché au terme de donnée renvoie à une « *information codée, figée et transmissible* ». Elle doit être « codée » : elle doit prendre une forme abstraite, correspondre à un certain référentiel pour pouvoir être collectée et croisée avec d'autres données présentant le même format. Par exemple, une date de naissance se présente conventionnellement sous la forme *jj/mm/aaaa* et peut être comparée une autre date de naissance, qui reprendra ce même référentiel. La donnée est « figée » : elle ne peut donc pas évoluer, sans quoi sa collecte et son traitement ne pourraient avoir lieu. Deux dates de naissance sont des données constantes, elles retracent un événement particulier, qui n'évoluera pas. Enfin, la donnée est « transmissible » : elle peut être enregistrée ou stockée puis déplacée de son support matériel vers un nouveau en vue de son traitement.[3]

La définition du « caractère personnel » pouvant être attaché à certaines données se retrouve à l'article 2 de la directive de 1995.[4] Elle est reprise à l'article 2 de la loi « Informatique et libertés ».[5] Ceux-ci indiquent que « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Il s'agit là d'une conception large prenant en compte les réalités des procédés de traitement et les possibilités de ré-identification de l'individu. Celle-ci peut être opérée par le responsable du traitement lui-même, par la réunion de différents responsables de traitement centralisant les données en leur possession, ou encore par une autorité publique procédant à des croisements de fichiers. Par ailleurs, les données personnelles « *nous définissent, reflètent parfois à notre insu, notre personnalité, nos goûts, nos aspirations, nos préoccupations, notre vie privée* »[6].

Initialement, les dispositions de la loi « Informatique et libertés » ne visaient que les « fichiers » recueillant des données à caractère personnel. Elles sont désormais élargies aux « traitements »

---

[3] *Éric PERES, « Les données numériques : un enjeu d'éducation et de citoyenneté » (avis du Conseil économique, social et environnemental), Journal Officiel de la République française, janvier 2015, p. 10*

[4] *Directive 95/46/CE 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*

[5] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

[6] *Éric PERES, « Les données numériques : un enjeu d'éducation et de citoyenneté » (avis du Conseil économique, social et environnemental), Journal Officiel de la République française, janvier 2015, p. 12*

qui pourraient être faits de ces données, le fichier en lui-même n'en représentant qu'un aspect restreint. Par exemple, les données qui circulent sur Internet ne forment pas, en soi, un fichier. L'article 2, alinéa 3 de la loi « Informatique et libertés » définit ainsi la notion de « traitement de données à caractère personnel » comme « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* ». Finalement, toute opération mettant en jeu des données personnelles peut être qualifiée de « traitement ».

Enfin, la notion de « responsable de traitement » désigne, au sens de l'article 3 de la loi « Informatique et libertés », « *la personne, l'autorité publique, le service, ou l'organisme qui, détermine ses finalités et ses moyens* ». Le responsable de traitement est donc celui qui dispose d'un pouvoir décisionnel sur l'ensemble des aspects du traitement.

Révolution numérique et traitement des données personnelles :

Durant les années 1990, l'Internet restait un outil à « taille humaine ». En effet, les résultats des requêtes provenaient de l'avis d'experts humains. Aujourd'hui, une même recherche peut renvoyer à des millions de sites web. Cette expansion a eu pour conséquence le développement d'un traitement global et automatisé des données. Qui plus est, les technologies numériques ont entrainé un bouleversement dans notre rapport à l'information. Les lieux de stockage de données tangibles, comme les bibliothèques ou les archives, commencent à présenter leurs limites en termes de capacité et d'attractivité, notamment. La réduction drastique des coûts de stockage et l'automatisation du traitement des données ont introduit des modifications structurelles dans l'accès à l'information.

Pour illustrer cette réduction des coûts de stockage, on peut indiquer qu'en 1980, un mégaoctet coûtait environ 300$ alors qu'il ne coûtait plus que 0,00022$ en 2014. Il s'agit alors de « mémoires numériques ». D'un autre côté, la production de données s'est également développée de manière spectaculaire du fait de l'accessibilité de l'Internet, de la généralisation de l'équipement informatique, des smartphones, du web 2.0 et du commerce électronique.

Ainsi, selon Eric Schmidt[7], il fallait, en 2011, deux jours pour créer un volume de données supérieur au volume de données créé entre l'origine de l'humanité à 2003.

Longtemps, collecte et traitement des données étaient liés aux pouvoirs publics (sondages, expertises publiques, renseignements, administration, services publics, etc.). Aujourd'hui, les données sont également collectées et utilisées par de très nombreux organismes privés. Les données sont alors créées par les individus eux-mêmes sur Internet, ou par l'intermédiaire de services associés à des objets dotés de capteurs, dits « connectés ». Ceux-ci s'inscrivent dans le cadre du « Life hacking » ou « prise de contrôle de l'existence » qui implique l'utilisation d'objets connectés pour simplifier le quotidien.

De grandes quantités de données sont alors transmises. Elles peuvent concerner l'alimentation, les divertissements, les déplacements, l'éducation, la santé, etc. Le développement des objets connectés conduit à un accroissement exponentiel du volume de données produites par les individus et captées par les organismes de traitement. Or, la sensibilité des données concernées pourrait engendrer d'importantes problématiques pour la vie privée des individus. Ainsi, le Conseil économique, social et environnemental (CESE) estime que « *la capacité qui sera donnée aux citoyens de maîtriser ces nouveaux flux de données pourrait devenir l'une des caractéristiques les plus cruciales de l'architecture informationnelle de nos sociétés* ».[8]

La valeur totale des données personnelles des citoyens européens représenterait la valeur de 330 milliards d'euros par an pour les organisations publiques et privées (gains de productivité, conquête de nouveaux marchés, etc.). La libéralisation de l'usage de ces données amènerait également un gain potentiel estimé à 670 de millions d'euros par an pour les consommateurs (gains de temps et baisse des prix).[9] Mais cela pourrait provoquer des conséquences désastreuses sur les libertés fondamentales des individus. Par conséquent, on assiste à une demande croissante de protection des données personnelles sur le territoire européen.

---

[7] Eric Schmidt a été le PDG de Google Inc. De 2001 à 2011, il en est actuellement le président exécutif du Conseil d'administration

[8] Éric PERES, « Les données numériques : un enjeu d'éducation et de citoyenneté » (avis du Conseil économique, social et environnemental), Journal Officiel de la République française, janvier 2015, p. 7

[9] Etude du Boston Consulting Group, The Value of our digital identity », publiée en 2012

Pour le secteur industriel, les données personnelles représentent une opportunité considérable en termes de valorisation à des fins publicitaires, d'études des comportements d'achat et de création de nouveaux services, de plus en plus adaptés aux besoins des consommateurs. Leur potentiel de valorisation est énorme. Ainsi, pour les entreprises du secteur numérique, le principal critère de valorisation n'est pas le chiffre d'affaires, ni la rentabilité mais réside dans le croisement de leur capacité à attirer le public et à recueillir des données personnelles. C'est ainsi que certaines start-up, dites « Licornes », sont valorisées à plus d'un milliard de dollars avant même leur introduction en bourse. Dans le domaine de la publicité, l'exploitation des données personnelles permet de toucher avec précision des individus susceptibles d'être intéressés par les produits ou services concernés. Les campagnes peuvent donc être ajustées à leurs cibles réelles. Ce qui les rend plus efficaces et permet d'économiser les frais de campagnes « globales » (par exemple, le prix d'achat de 30 secondes d'antenne, en heure de prime, sur TF1[10] ou Canal +[11] varie entre 20.000€ et 68.000€ en temps normal). Cette flexibilité permet d'ouvrir le marché à des entreprises plus petites (TPE et PME). D'une manière générale, l'exploitation des données personnelles permet aux acteurs industriels d'ajuster au mieux l'offre à la demande. L'entreprise la plus compétitive sera alors celle qui aura le mieux anticipé les besoins du consommateur et qui lui aura fourni les biens ou services les plus adaptés à ses attentes.

La mise en place progressive d'une régulation des traitements de données personnelles :

Face à ces modifications affectant l'ensemble de nos sociétés, une régulation du traitement des données personnelles a très vite émergée, que ce soit à l'initiative du législateur national, ou européen.

En France, le scandale provoqué par l'affaire SAFARI a fait prendre conscience au pouvoir législatif de la nécessité de contrôler les fichiers centralisant des données. Le Ministère de l'intérieur avait lancé, en 1973, un système automatisé pour les fichiers administratifs des citoyens français. L'objectif était d'y centraliser tous les fichiers nominatifs de l'administration française : registre de l'état civil, cadastre, fichiers des impôts, fichier du Ministère du travail, etc. Ce projet a été révélé au grand public par le journal Le monde en 1974. La mobilisation de

[10] *Voir : http://www.tf1pub.fr/offres/grilles/TF1/TF1*

[11] *Voir : http://www.canalplusregie.fr/tarifs/canal/tarifs-classiques-121*

l'opinion publique a abouti à la création de la CNIL pour encadrer ce système, puis à l'adoption de la loi « Informatique et libertés » par le Parlement. Initialement, la loi visait principalement les traitements opérés par la sphère publique. Pour illustrer les progrès technologiques réalisés depuis, l'ordinateur « Iris-80 » dont s'était pourvu le Ministère de l'intérieur était à l'époque dépeint comme ayant une « effrayante capacité de stockage ». Celle-ci était en réalité de seulement 2Go, ce qui représente la taille d'une « petite » clé USB aujourd'hui.[12]

De son côté, le droit européen n'est pas resté insensible à la protection des données personnelles et a souhaité procéder à son harmonisation dans l'ensemble de l'Union. L'objectif principal répondait à une logique économique : il s'agissait d'éviter d'éventuels problèmes de concurrence engendrés par des régulations nationales trop disparates. Ainsi, la directive de 1995 a vu le jour. Elle s'est très largement inspirée de la loi « Informatique et libertés », dont elle a repris de nombreux principes. A l'occasion de la loi de transposition du 6 août 2004,[13] le législateur a rééquilibré les dispositions « informatique et libertés » en faveur du secteur privé. Désormais, la loi assure une égalité entre le secteur public et privé dans la procédure entourant le traitement. Cette égalité est cependant mise de côté dans les domaines relevant de la souveraineté, qui ne relèvent pas de la compétence de l'Union. La protection est alors axée autour de la sensibilité des données, que celles-ci proviennent de la sphère publique ou privée n'a aucune importance. Par ailleurs, le législateur a également renforcé le rôle de la CNIL, qui se voit depuis dotée d'un pouvoir de sanction envers le secteur privé.

Par ailleurs, le législateur européen a également publié, en décembre 2000, un règlement visant à réguler les traitements de données personnelles opérés par les institutions communautaires. [14] En effet, celles-ci sont amenées à partager un grand nombre de données personnelles dans le cadre de leurs compétences, notamment la Commission européenne. Ce règlement vise à assurer une protection aux citoyens européens face aux flux « institutionnels » de données.

---

[12] *Philippe Boucher, « SAFARI, ou la chasse aux français », Le Monde, 21 mars 1974*

[13] *Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

[14] *règlement (UE) n° 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données*

Le règlement a pour effet d'exiger des institutions européennes la même protection des données que celle imposée aux responsables de traitement européens « normaux ». Il reprend ainsi la majeure partie des dispositions de la directive de 1995. Les traitements visés ici sont régulés par le Contrôleur européen de la protection des données (CEPD) et chaque organe ou institution européenne doit désigner un délégué assurant un lien avec l'autorité de contrôle.

Le développement du « Big Data » :

Le « Big Data » est un traitement particulier des données qui présente la caractéristique d'obéir à la « règle des trois V ». Le premier « V » correspond au « volume ». En effet, l'intérêt du « Big Data » réside dans sa capacité à traiter des quantités considérables de données. Les masses de données à traiter observent une croissance exponentielle. Le second « V » représente la « vélocité ». La collecte, l'analyse et l'exploitation des données doit se faire de manière quasi-immédiate, voire en temps réel dans des domaines sensibles comme le renseignement, la lutte antiterroriste, la surveillance du territoire, etc. Le troisième « V » correspond à la « variété » : les données traitées peuvent revêtir des formes et des structures très variées. S'ajoutent à ces trois « V » deux autres caractères définissant le « Big Data ». Ainsi, la « valeur » représente un aspect technique de l'utilisation des données. Par exemple, la manière dont elles peuvent être converties pour transmettre l'information recherchée. Et enfin, la « véracité » ou la « pertinence » des données. Celle-ci revêt une importance capitale dans le traitement automatisé. En effet, des données erronées peuvent compromettre l'ensemble de l'analyse, c'est ce que l'on appelle le « Bug data ». On peut illustrer ce phénomène par le faux Tweet concernant un prétendu attentat à la maison blanche qui aurait touché directement le Président Obama. Ce canular a provoqué un vent de panique à Wall Street : les logiciels ont déclenché des ventes massives de titres boursiers à l'analyse des mots clés « Obama, White House, Bomb, Attack, etc. ».[15]

Pour résumer, le « Big Data » consiste à stocker et traiter en temps réel des volumes considérables de données très variées (forme, provenance, structure, etc.). Il permet de croiser et d'enrichir les données de manière très rapide. On entre alors dans une logique d'anticipation, permettant l'expression de « modèles prédictifs ». Sur Internet, on retrouve l'expression du

[15] *Eric Sergheraert, « L'utilisation du Big Data dans le secteur pharmaceutique : des promesses indéniables mais aussi des obstacles juridiques potentiels », Propriétés intellectuelles, avril 2016, n° 59, p. 181*

« web sémantique », qui exprime le fait d'utiliser les métadonnées[16] fixées sur l'ensemble des ressources du web et de les exploiter par l'intermédiaire d'un traitement de type « Big Data ». Le « Big Data » induit le renversement de la logique cartésienne consistant à observer la corrélation de certains événements et à en tirer des conséquences quant au lien de causalité qui les unit. La réflexion et la logique humaine sont basées sur l'analyse de la causalité, de même que la recherche scientifique. Ainsi, la coïncidence est prise en compte pour pouvoir être retirée du processus décisionnel. Le traitement automatisé de masses informationnelles opère un glissement de la prédiction causale vers une prédiction statistique. Pour schématiser : lorsque deux évènements sont liés, on ne cherche plus à en comprendre la causalité mais à en prédire l'occurrence. Si l'un survient, on sait que l'autre ne tardera pas à suivre. Chacune de ces approches admet ses propres limites.

L'approche causale isole un événement par le lien de causalité. C'est-à-dire que la réalisation du second événement ne peut s'expliquer que par le lien qui l'unit au premier. La cause est alors déterminante. Mais l'analyse peut être biaisée en cas d'erreur dans le choix de la cause déterminante. D'autre part, elle peut s'avérer incomplète lorsqu'elle omet de prendre en compte d'autres facteurs - qui échappent à l'analyste ou qui lui sont inconnus - pouvant jouer un rôle important dans la réalisation de l'événement. De son côté, l'approche statistique ignore l'explication « logique », donc l'étude du lien de causalité. Elle permet donc de prédire la survenance d'événements mais ne s'encombre pas à chercher à l'expliquer. L'analyse, basée sur le traitement d'information, ne concerne alors que des événements « connus », ayant été incorporés à la base de données. Si cette approche est plus efficace dans l'analyse de phénomènes récurrents, elle se retrouve stérile lorsque des éléments nouveaux se produisent.

La solution pour pallier les limites propres à chaque approche est de les réunir autour d'une même analyse. On peut alors choisir d'allier les capacités de l'homme à celles de la machine (développement d'interfaces homme-machine). On peut également décider de créer une machine capable d'adopter les deux systèmes d'analyse, ce qui nous rapprocherait considérablement de l'idéal de l'intelligence artificielle. Parvenir à une telle combinaison de la logique et de la statistique révolutionnerait le monde de la Recherche scientifique et ouvrirait à l'être humain des perspectives à peine imaginables.

---

[16] *La métadonnée est une nouvelle structure de l'information, essentielle au traitement de données, qui en assure la description. Elle décrit, explique, localise ou facilite la découverte, l'utilisation ou la gestion d'une ressource informationnelle.*

En résumé, les traitements de type « Big Data » anticipent par la statistique, ils ne s'embarrassent pas de savoir pourquoi ou comment des corrélations ont lieu. L'anticipation est ici le fruit de probabilités. Ainsi, un événement arrive car il est fortement possible qu'il se produise. Un tel calcul à partir de données si sensiblement différentes (zone géographique, nature de la donnée, structure et forme de celle-ci, information véhiculée) ne peut être accompli que par la voie informatique.

Un outil de calcul d'une telle puissance peut avoir des applications considérables et innovantes dans des secteurs aussi variés que l'étude de l'environnement et des phénomènes climatiques ; l'agriculture (où le numérique permet de rationnaliser et d'augmenter la productivité : automatisation de l'irrigation, installation de capteurs au sol, etc.)[17] ; l'urbanisme (où des villes connectées comme celle de Santander en Espagne permettent aux services publics de s'adapter en temps réel aux besoins des administrés : parking, chaleur, bruit, passage des véhicules, etc.) ; l'énergie (utilisation de l'énergie en P2P, distribution en temps réel, développement de réseaux intelligents, etc.) ; le marketing (anticipation de comportements consuméristes, études de marché, profilage, adaptation de la production, etc.) ; les conflits armés (prise de décision en fonction de l'environnement, de la position des cibles, de la présence de civils, etc.) ; l'intelligence nationale et la surveillance du territoire ; etc. Bien d'autres domaines sont concernés par les promesses du « Big Data ».

Les perspectives du « Big Data » en matière de santé :

Celui-ci a fait naître des attentes considérables dans le domaine de la santé, où l'analyse massive de données permet d'adopter une approche davantage basée sur l'anticipation, la prévention et la surveillance. L'analyse et le croisement de données relatives au génome humain ou animal ou bien encore de dossiers médicaux, notamment, permettront à la médecine de s'adapter de plus en plus à l'individu. Les potentiels du traitement des données personnelles sont énormes dans le domaine de la santé. Ainsi, les partenariats entre les grandes entreprises du numérique et les laboratoires pharmaceutiques ne cessent de se développer, à l'instar de Google qui s'est rapproché de Biogen et de Sanofi. Une telle proximité traduit le besoin de l'industrie de la santé d'accéder à de plus amples informations sur les patients, de profiter de la collecte et de l'exploitation des données pour améliorer l'offre de soins. Ainsi, on peut observer une très nette

[17] Par exemple, le projet de l'ONG américaine « The Nature Conservancy » a permis de réutiliser l'eau de pluie et de préserver un milliard de litres d'eau en deux ans

augmentation des données de santé créées par le biais d'applications (6.000 applications en 2010 ; 100.000 en 2013). De plus, si près de 15 milliards d'objets connectés sont disséminés à travers le monde aujourd'hui, ce nombre est estimé à 80 milliards d'ici 2020.[18] Ainsi, le médecin américain Eric Topol estime qu' « *excepté pour certaines fonctions clés comme les soins intensifs et la chirurgie, les hôpitaux seront entièrement transformés en centres de surveillance des données. Les gens souriront en repensant aux visites chez leur médecin avec le légendaire stéthoscope ainsi que l'ensemble des pratiques qui existaient avant l'ère numérique* ».[19]

L'analyse massive de données, qui n'en est qu'à ses prémices, admet cependant des limites conséquentes dans ses résultats. Ainsi, Google avait en 2008 imaginé un algorithme censé prédire le développement de la grippe H1N1 en postulant que les personnes infectées en rechercheraient les symptômes sur le moteur de recherche. Il s'agissait ainsi de traiter les recherches effectuées par les usagers en fonction des mots clés utilisés lors des épidémies passées. Cette méthode qui semblait très prometteuse s'est pourtant soldée par un échec de taille : l'algorithme n'a pas permis de prédire l'occurrence de l'épidémie de 2009. Il a, par contre, surestimé le développement de la maladie au cours du temps.[20]

Mais cet échec ne freine en rien les travaux des médecins et des scientifiques sur les systèmes d'analyse massive. Ainsi, dès 1970, des travaux avaient démontré l'importance des déplacements par avion dans la propagation de la pandémie de grippe espagnole. L'entreprise « Gleam » a donc mis en place un système d'étude des flux aéroportuaires, couvrant plus 50 millions de vols chaque année et étudiant les connexions de 3.800 aéroports. 99,9% du trafic mondial y est représenté. Ce modèle démontre une grande efficacité dans l'étude de la propagation de certaines maladies virales, comme par exemple la grippe H1N1, Ebola, le Chikungunya, etc. De la même manière, le suivi des déplacements des personnes à l'aide de leurs téléphones portables permet, à une échelle plus restreinte, de comprendre le développement d'épidémies. C'est ce procédé qui a été utilisé pour comprendre les

---

[18] *Rapport de l'Institut de l'audiovisuel et des télécommunications en Europe (IDATE), « The Internet of Things », publié le 26 août 2013*

[19] *Eric Topol, « On The Future Of Medecine », Wall Street Journal 7 juillet 2014*

[20] *Jean-Yves NAU, « Santé et Big Data: l'échec de Google Flu ne doit pas cacher la forêt » : http://www.slate.fr/story/120441/sante-big-data-echec-google-flur.*

conséquences sanitaires de la catastrophe survenue à Haïti en 2014 et le développement du choléra dans la ville de Port au Prince parmi les victimes du séisme.[21]

Cependant, les données susceptibles d'intéresser l'industrie de la Santé ne se limitent pas aux seules données médicales, définies à l'article 4 du Règlement européen du 27 avril 2016 comme des « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de service de soins de santé qui révèlent des informations sur l'état de santé de cette personne* ». Ces données doivent être entendues au sens large comme un ensemble d'informations pouvant être recueillies dans le cadre médical. Elles englobent alors les données génétiques, les échantillons biologiques, ou bien les données relatives à une maladie, un handicap, un risque de maladie.[22]. L' « Internet des objets » englobe également les données « bien-être », permettant le « Quantified self » (la mesure de soi-même) ainsi que le « Quantified home » (la mesure de l'environnement dans lequel l'individu évolue). Ces données concernent les habitudes des individus (heure de lever et de coucher, mesure du poids, pratiques sportives, alimentation, etc.). Contrairement aux données de santé, elles sont très peu règlementées. En effet, la CNIL estime que ces données sont recueillies sur la base du volontariat. Le consentement des personnes concernées étant obtenu, l'exploitation de ces données échappe à tout contrôle particulier et ne nécessite aucune autorisation préalable au traitement.[23]

L'extension de la notion de données de santé à ces données « bien-être », dont l'utilité - et donc la valorisation - pourrait s'accélérer avec le développement des technologies du numérique, serait un frein considérable pour le « Big Data » mais ne semble pas être d'actualité pour le moment. Il faudra bien pourtant protéger ces données et prendre en considération l'influence que leur traitement pourra avoir, dans un avenir proche, sur les libertés fondamentales des citoyens européens.

---

[21] *Pierre-Yves Boelle, Rodolphe Thiébaut et Dominique Costagliola, « Données massives, vous avez dit données massives ? », Questions de santé publique n° 30, septembre 2015, p. 2*

[22] *Considérant 26 du règlement européen du 27 avril 2016*

[23] *Eric Sergheraert, « L'utilisation du Big Data dans le secteur pharmaceutique : des promesses indéniables mais aussi des obstacles juridiques potentiels », Propriétés intellectuelles, avril 2016, n° 59, p. 183*

Ainsi, la mise en œuvre de tels traitements par le secteur prudentiel pourrait devenir une préoccupation majeure des autorités de régulation. En effet, le « Big Data » pourrait amener les données, même anodines, à être incluses dans des process d'évaluation des risques de santé. Cela reviendrait à opérer un profilage de l'individu en fonction des risques qu'il présente. Par exemple, l'analyse des habitudes alimentaires, des pratiques sportives, des statuts postés sur les réseaux sociaux, des recherches de symptômes sur un moteur de recherche ou la fréquence de ces recherches, pourrait amener les compagnies d'assurance à « faire parler » ces données. Les données ainsi traitées ne seraient alors plus anodines et donneraient une quantité d'informations considérable sur l'état de santé d'une personne.

Dans cette logique, les données stockées dans le SNIRAAM[24] représentent l'une des plus grandes concentrations administratives de données au monde. Ces données sont collectées à chaque fois qu'un individu à des rapports avec un organisme de santé sur le sol français. L'accès à ces données était jusqu'ici très restreint, n'étant que partiellement ouvert aux organismes de recherche publique. Mais le Conseil d'Etat en a récemment ouvert l'accès aux organismes privés, sous certaines conditions (notamment la nécessité de réaliser une étude d'intérêt général)[25]. La haute juridiction administrative a en effet jugé que les dispositions « informatique et libertés » ne prévoyaient pas une restriction d'accès à ces données aux opérateurs privés. Face à cette décision, les demandes d'accès aux données de santé des citoyens français risquent très fortement d'exploser. À côté des résultats bénéfiques que pourrait entrainer une ouverture d'accès aux données du SNIRAAM (évaluation des politiques de santé, amélioration de l'offre de soin, étude des maladies et de l'efficacité des traitements, surveillance accrue de la sécurité sanitaire, etc.), on pourrait craindre leur appropriation et leur traitement pour des motifs moins louables. Il serait ainsi à craindre, malgré les prévoyances législatives, que ces données soient utilisées pour influencer l'accès des individus aux contrats d'assurance ou pour en déterminer les cotisations.[26]

---

[24] *Système national d'information inter-régimes de l'Assurance-maladie*

[25] *Arrêt du Conseil d'Etat, 1ère – 6ème chambres réunies, 20 mai 2016, n° 38-5305, Celtipharm c/ Ministère des affaires sociales et de la santé*

[26] *Cécile THIBERT, « Les données personnelles de santé accessibles aux assurances et laboratoires » : http://sante.lefigaro.fr/actualite/2016/05/30/25032-donnees-personnelles-sante-accessibles-assurances-laboratoires*

L' « Internet des objets » : le futur du « Big Data » :

L'intégration des objets connectés dans le quotidien représente le futur du « Big Data ». Ces objets dotés de capteurs emmagasinent des informations sur le quotidien : mode de vie, centres d'intérêts, goûts. Ainsi, on peut prendre l'exemple de Google, qui a racheté la compagnie Nest Labs pour 2,3 milliards d'euros en 2014. Cette compagnie commercialise des thermostats intelligents qui enregistrent les habitudes des utilisateurs pour leur proposer des programmes personnalisés contrôlant la température de l'habitat.

Les données recueillies par les appareils connectés sont très variées, produites de manière continue et collectées de manière instantanée en très grande quantité, ce qui les inscrit donc dans le cadre des traitements de type « Big Data ». La valorisation de ces données peut être considérable mais elle est nécessairement liée aux traitements qui en seront faits. Ainsi, on peut douter du fait que leur traitement se limitera à la simple personnalisation du service proposé ou à son amélioration. On peut alors envisager la construction de bases de données considérables à des fins de profilage ou de ciblage publicitaire. Par ailleurs, dans le cadre du phénomène de « datafication », visant à transformer en information les interactions des individus avec tout ce qui les entoure, il est fortement probable que les données personnelles soient couplées à d'autres bases de données provenant des réseaux sociaux, du commerce électronique, de fichiers publics, etc. Cela peut poser d'énormes problèmes en termes de vie privée et altérer de manière considérable les libertés fondamentales garanties aux citoyens européens.[27] Même si les entreprises du numérique se conformaient à une certaine éthique « informatique et libertés » (respect des dispositions légales et mise en place d'une protection de la vie privée dès la conception de l'objet connecté), demeureraient également les risques induits par la cybercriminalité. Le piratage des données personnelles des utilisateurs pourrait conduire, par exemple, à savoir à quel moment des résidents sont ou non présents à leur domicile, à pouvoir ouvrir des serrures synchronisées, à désactiver à distance les freins d'une voiture électrique, à pirater des bases de données du responsable de traitement et à capter des données collectées, etc.

En l'absence de statut juridique de l'objet connecté, des questions se posent, notamment en ce qui concerne le consentement des utilisateurs à la collecte et à l'exploitation de leurs données.

---

[27] Caroline Laverdet, « La sécurité des données à l'ère des objets connectés », Expertises des systèmes d'information, juin 2014, pages 214 à 217

Certains évoquent un « droit à la désactivation » qui donnerait la possibilité aux individus ne souhaitant pas partager leurs données personnelles de couper les puces électroniques de leurs appareils pour laisser place au seul usage « traditionnel » du produit. Ainsi, une balance, un frigo, un chauffage, une montre ne serviraient respectivement qu'à peser, réfrigérer, chauffer une pièce et donner l'heure sans pour autant s'adapter aux habitudes de l'utilisateur et, surtout, sans les transformer en informations. Ce droit n'est pas encore envisagé par les législateurs français ou européens. Toutefois, il peut se matérialiser par l'incorporation d'un bouton « silence » directement sur les appareils et ce, dès leur conception. Cela permettrait de mieux l'adapter à la volonté de son propriétaire qui pourrait alors décider, quand il le souhaite, de profiter des capacités de « connexion » de l'appareils. Un tel dispositif entrerait dans le cadre du « Privacy by Design », qui est fortement encouragé par les institutions européennes, comme nous aurons l'occasion de le détailler plus tard.

« Open Data », la recherche de la « Performance publique » :

L' « Open Data » est un mouvement consistant à publier les données collectées par les organismes publics. Les données concernées ne sont pas nominatives (rendues anonymes) et ne relèvent donc pas, en règle générale, de la vie privée. Deux principes sont à l'origine de ce phénomène : la disponibilité des données détenues par l'administration (qui implique un accès libre pour tous) et la possibilité offerte aux citoyens et au secteur privé de les réutiliser. L' « Open Data » est un vecteur d'innovations économiques, sociales, environnementales et démocratiques. En effet, la publication des données par l'administration est un instrument de transparence et pourrait favoriser la confiance et l'implication des administrés dans le fonctionnement de la collectivité. D'autant plus que celui-ci pourrait en être grandement amélioré (allégement des procédures administratives, réduction des coûts, etc.). Des réserves se font toutefois sentir quant à l'objectif de transparence et de participation citoyenne. En effet, les données rendues publiques ne permettent pas, en elles-mêmes, la captation d'une information par l'administré. Celui-ci a besoin de recourir à un intermédiaire pour donner un sens à ces données. De même, le besoin de logiciels payants pour lire certains formats de données remet en cause la gratuité de la mise en ligne des données. Ce manque de lisibilité pour l'administré déplace les données publiques dans une logique plus commerciale, ciblant davantage le secteur privé. Quoi qu'il en soit, l'« Open Data » favorise le développement de

services innovants dans l'intérêt du public et contribue au « rayonnement économique » des collectivités territoriales.[28]

Ce mouvement a été initié par l'adoption de circulaires administratives. Plus tard, la loi « CADA »[29] a posé le principe selon lequel toute personne peut avoir accès aux documents détenus par l'administration dans le cadre de sa mission de service public. Son article 1er consacre le « *droit de toute personne à l'information* » et reconnaît « *la liberté d'accès aux documents administratifs* ». Il s'agit d'un droit d'accès individuel qui ne prévoit pas la possibilité pour les administrés de réutiliser les données. Par la suite, la transposition de la directive « PSI »[30] a rendu possible la réutilisation des informations publiques à des fins autres que celles pour lesquelles elles sont élaborées ou recueillies. Face aux dangers que représentent les évolutions technologiques dans le domaine du numérique, celle-ci a été modifiée par une nouvelle directive, dite « PSI 2 ».[31] La loi de transposition de cette nouvelle directive[32] impose la publication des données émanant d'établissements culturels et de recherche. Cependant, les données ne devront pas concerner des travaux en cours, non divulgués ou faisant l'objet de droits de Propriété intellectuelle pour ces établissements.[33]

L' « Open Data » connaît une croissance fulgurante et tend à devenir une obligation pour l'administration. Certains sont en faveur de l'introduction légale d'une obligation, pour l'ensemble des pouvoirs publics, de mettre à disposition, sur Internet, les données qu'ils ont pu recueillir. En ce sens, l'article 29 du Projet de loi de développement des solidarités territoriales et de la démocratie locale vise à rendre obligatoire la diffusion des données publiques pour les communes de plus de 3.500 habitants. Cela ne concerne, dans l'absolu, pas des données à caractère personnel. En effet, la plupart des informations du secteur public mises à disposition

---

[28] *Jérôme Lefort, Marion Hainez et Marine Chatelet, « Gérer, sécuriser et valoriser ses données personnelles des collectivités territoriales », Territorial Editions, 2015, p. 93*

[29] *Loi n°78-753 du 17 juillet 1978 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal*

[30] *Directive 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public*

[31] *Directive 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public*

[32] *Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public*

[33] *Céline Castets-Renard, « La transposition de la directive PSI 2 et l'ouverture des données publiques », Dalloz IP/IT 2016, p. 6*

des internautes sont exemptes de données personnelles. Elles sont, par exemple, relatives aux horaires et localisations des services, aux évènements culturels et sportifs, à l'environnement, au tourisme, etc. Cependant, l'administration dispose également de nombreuses données à caractère personnel. Ces données ne peuvent être publiées sur Internet sans qu'un niveau de sécurité suffisant ne soit assuré quant à leur anonymat, conformément à l'article 13 de la loi « CADA ». Toutefois, la réutilisation des informations publiques peut permettre, par leur recoupement, la ré-identification des personnes concernées sans même renfermer un contenu identifiant. C'est donc l'usage fait de la donnée publique qui devrait lui conférer son caractère personnel. Une transparence absolue de l'administration ne semble alors pas souhaitable au regard de la protection de la vie privée des citoyens. Par ailleurs, la réutilisation des informations publiques comportant des données personnelles est soumise au respect des dispositions de la loi « informatique et libertés » au même titre qu'un traitement de données privées.

Le monde numérique et les rapports à l'information connaissent ainsi des évolutions considérables : puissance des moteurs de recherche, capacités d'analyse, développement du « Big Data », croissance de la création de données par les individus sur le web ou par l'intermédiaire d'objets connectés, dématérialisation croissante de l'administration, etc. La société civile apparaît très mitigée sur la question du numérique : si elle attend avec un grand optimisme des résultats positifs de ces nouvelles technologies (particulièrement dans les domaines de la santé, de l'environnement, de l'énergie ou dans l'amélioration de la vie quotidienne), elle en appréhende également les usages et finalités ainsi que les risques qui en découlent pour les libertés fondamentales. Or, la démocratie n'est viable et réelle qu'à la condition d'être soutenue par l'Etat de droit.

Les institutions européennes sont alors amenées à se demander comment, à l'aube de l'ère de l'information, concilier la protection des libertés fondamentales des citoyens européens et le développement de l'économie de la donnée personnelle, véritable clé de voûte du secteur numérique.

Depuis le Traité de Lisbonne de 2006, la protection des données à caractère personnel est élevée au rang des droits fondamentaux de l'Union européenne. Elle se trouve donc consacrée à l'article 16 TFUE et à l'article 8 de la CEDH.

Cette consécration « ultime » permet à l'Union de légiférer de manière spécifique dans ce domaine et d'avoir recours, pour ce faire, à son instrument normatif le plus puissant : le règlement européen. De très âpres négociations ont eu lieux entre les partisans de la protection des internautes et les lobbys des grandes entreprises du numérique, qui préféraient voir leur activité libéralisée au maximum. En effet, les lobbys ont été très actifs, notamment en ce qui concerne le secteur privé et les autorités américaines. Ainsi, cinq fois plus d'amendements ont été déposés par les lobbyistes lors de la construction du Projet de règlement pour la protection des données personnelles qu'à l'occasion des cinq directives du « Paquet télécom » en 2009 : près de 4.000 amendements ont été déposés.

Un accord a été trouvé entre le Conseil et le Parlement européen en décembre 2015. Il s'agit d'un compromis entre les deux institutions. Le conseil a adopté le Projet de règlement en première lecture le 8 avril 2016. Le Projet a ensuite été adopté par le Parlement le 16 avril 2016, ce qui a donné lieu à la publication du « Règlement général sur la protection des données »[34] (RGPD). Ce dernier reprend les principes fondamentaux de la protection des données personnelles : légalité, proportionnalité, adéquation de la collecte des données, limitation de la durée de conservation, détermination de la finalité du traitement, information et consentement des personnes concernées, interdiction de l'exportation des données hors UE, etc.

Le règlement a pour vocation d'unifier la protection des données personnelles sur l'ensemble du territoire européen et de l'adapter à la Révolution numérique. Il s'oriente autour de quatre axes principaux : renforcer les droits des individus ; mettre en place des mécanismes organisationnels assurant le respect de la protection des données en éloignant l'obsolescence des dispositions ; construire une politique européenne cohérente pour les autorités de protection et prendre en compte le caractère mondial de la protection des données.[35]

Par ailleurs, des problématiques comme celles de l'autonomie de la volonté en matière de traitement des données personnelles, l'exercice du droit à l'oubli, les dérives sécuritaires et la

[34] *Règlement (UE) n° 2016/679 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*

[35] *Marc Lemperière, « Données personnelles : les dernières évolutions du règlement communautaire, Expertises des systèmes d'information, janvier 2014, page 14 »*

surveillance de masse, sont révélatrices d'une fracture majeure : la perte de confiance de l'individu dans la société et, plus particulièrement, dans l'environnement numérique. Face à la prise de conscience par l'opinion publique des dangers qui pesaient sur les libertés individuelles, les institutions européennes se sont également attachées à promouvoir la confiance des citoyens européens dans le secteur numérique (« Digital trust ») et à leur redonner une certaine maîtrise de leurs données personnelles. Cette logique passe autant par l'adoption d'une approche pédagogique et par la diffusion d'une « culture numérique » que par l'implication du secteur privé dans le processus de régulation. Celui-ci est également victime de cette crise de confiance. Ainsi, les acteurs privés doivent, eux aussi, apporter leur contribution à son bon fonctionnement.

Certes, le développement du numérique ne peut se faire au détriment de la personne et de ses droits les plus fondamentaux mais une trop grande précaution face à ces nouvelles technologies ne doit pas conduire l'Union européenne à « rater le train » de l'ère numérique. En ce sens, les négociations commerciales avec les Etats-Unis en matière de données personnelles apparaissent comme une obligation et le tout récent Privacy Shield, comme une nécessité.

Si les institutions européennes viennent renforcer les obligations pesant sur le responsable de traitement et les droits des personnes concernées, renforçant la protection des données personnelles (**1ère Partie**), elles adoptent également une logique économique en essayant de promouvoir leur intégration dans le marché du numérique (**2nde Partie**).

Partie 1 - Harmonisation de la protection des données personnelles dans l'UE.

Centraliser des données personnelles en vue d'en réaliser le traitement n'est pas un phénomène récent. Déjà, au XVIII^{ème} siècle, la Préfecture de Police de Paris avait constitué un fichier manuel recensant des millions de fichiers relatifs aux criminels. De son côté, la notion de vie privée est un concept relativement récent. Inconnue dans l'Antiquité, elle apparaît durant le XIX^{ème} siècle dans les pays ayant bénéficié de la Révolution industrielle. Il s'agissait déjà, à cette époque, de protéger la vie privée et le droit à l'intimité contre les intrusions de la technologie de cette époque (photographie, microphone, …). Cependant, à partir des années 1970, l'apparition de l'informatique a conduit à ce que les fichiers puissent être informatisés et industrialisés. C'est également au cours de cette période que le concept de vie privée devient une priorité politique en France, de par son introduction à l'article 9 du Code civil. Ce n'est pourtant qu'en 1999 que le Conseil Constitutionnel a rattaché le droit au respect de la vie privée au « droit à la sûreté » porté par l'article 2 de la Déclaration des droits de l'homme et du citoyen. De surcroît, il a fallu attendre le Traité de Lisbonne pour que ce principe soit reconnu, au rang européen, comme un droit fondamental de la personne et qu'il apparaisse dans le Traité sur le fonctionnement de l'Union européenne (article 16). C'est donc bien tardivement que la notion de vie privée est sacrée au plus haut niveau de la hiérarchie des normes.

Par ailleurs, la notion de vie privée est une notion relative, qui peut s'effacer devant certains impératifs comme la liberté d'expression ou l'intérêt public. Le Tribunal de grande instance de Paris a ainsi pu indiquer que *« (…) ces droits peuvent cependant céder devant les nécessités de la liberté d'expression lorsque la diffusion des informations ou des images sont légitimes au regard de ces nécessités, l'appréciation de cette légitimité étant fonction d'un ensemble de circonstances tenant à la personne qui se plaint de l'atteinte aux droits protégés, par l'article 9 du Code civil, notamment en sa qualité et son comportement antérieur, l'objet de la publication en cause, son contenu, sa forme, l'absence de malveillance et d'atteinte à la dignité de la personne, ainsi que sa participation à un débat d'intérêt général* ».[36]

[36] *TGI Paris, 17ème chambre, 13 novembre 2013*

La définition de la vie privée n'est elle-même pas aisée à tracer. En effet, celle-ci n'est pas définie par le droit. Il faut alors se référer à une longue construction jurisprudentielle qui en fait, au fil des jugements, une notion très large. Elle englobe aussi bien le respect de l'intimité que celui des correspondances (quelle que soit leur forme), mais encore la protection contre les technologies de l'informatique ou bien le droit à l'image. Cette acception ne se retrouve pas forcément telle qu'elle sur d'autres continents : la vie privée est « question de culture ».[37] Cela contribue à expliquer les difficultés à mettre en place une protection internationale des données personnelles. Un consensus semble difficile à trouver autour d'une notion qui n'a pas la même valeur, la même signification ou qui ne correspond pas à la même réalité selon les Etats dans lesquels on se trouve. La construction du droit européen et sa diffusion - forcée - à l'étranger porte à se demander si l'Union européenne n'impose pas ses propres standards, sa conception culturelle de la vie privée, reprise ailleurs pour des impératifs d'ordre économique.

De manière synthétique, le droit à la vie privée consiste en l'absence de surveillance ou de divulgation d'informations relatives à ce que l'on fait, ce que l'on dit, ce que l'on aime ou non. Cela consiste également à avoir le droit de ne pas subir d'intrusions ou de discriminations en fonction de ces éléments d'intimité, que l'on ne souhaite pas divulguer. Toutes les données personnelles ne relèvent donc pas de la vie privée. Mais avec le développement du numérique et la fulgurance des nouvelles technologies, les données personnelles - et le traitement qui en est fait - sont susceptibles d'engendrer des intrusions considérables dans la vie privée des individus.

Face au lien étroit qui unit les notions de données personnelles et de vie privée, le législateur, français ou européen, a dégagé un certain nombre de principes dans le but d'apporter une plus grande protection à la collecte et au traitement de ces données. Ces principes constituent une sorte de « Déclaration des droits de l'homme » dans l'univers du numérique (Chapitre 1). D'autre part, des autorités de régulation ont été créées pour en vérifier la bonne application par les responsables de traitement. Celles-ci voient leurs prérogatives et leur participation au processus de régulation renforcées au fil du temps (Chapitre 2).

[37] *Vincent Gautrais, « Différences culturelles en matière de vie privée : point de vue canadien », Dalloz IP/IT 2016 p. 128*

Chapitre 1 : Les contours d'une « déclaration des droits de l'homme » à l'ère du numérique.

La consécration de la protection des données personnelles au rang de liberté fondamentale de l'Union européenne a conduit le droit européen à construire une régulation conséquente dans ce domaine. Toutefois, la transposition de la directive de 1995 par les Etats membres a donné naissance à 27 régimes juridiques différents. Ceci est à la fois source d'insécurité juridique pour les citoyens européens et pour les opérateurs du secteur du numérique, mais constitue également un frein considérable à la circulation de l'information sur le territoire européen. En effet, une directive donne des orientations qui doivent être respectées par les Etats membres. Elle fait l'objet d'une transposition dans le droit national par des lois devant en reprendre les principes. De ce fait, elle laisse une certaine marge de manœuvre aux législateurs nationaux et peut conduire à des disparités d'appréciation : on trouve alors autant de transpositions différentes qu'il y a d'Etats membres.

Pour favoriser l'homogénéité des régulations nationales en matière de données personnelles, la Commission a jugé bon de refondre la directive de 1995 à l'aide d'un instrument normatif plus incisif : le règlement. Celui-ci est directement applicable dans tous les Etats membres, qui ne disposent alors plus de la marge d'appréciation attachée à la transposition d'une directive. Ainsi, bien que les autorités nationales et les tribunaux disposent toujours d'une certaine marge de manœuvre pour interpréter les différentes dispositions du règlement, celui-ci va considérablement rapprocher les législations nationales dans l'ensemble du territoire européen. La protection s'en retrouvera donc plus cohérente et plus facile à appréhender pour les citoyens européens et pour les responsables de traitement. Par conséquent, suite à de longues négociations, le règlement général sur la protection des données (RGPD) a été publié le 27 avril 2016.

Le champ d'application du RGPD ne diffère pas de celui de la directive de 1995. Ainsi, tout comme l'article 2 de la directive, le règlement cible les « *traitements de données personnelles automatisés en tout ou partie* » ainsi que les « *fichiers automatisés* ». Il ne s'applique toutefois pas aux domaines régaliens réservés aux Etats membres, à savoir la poursuite et la répression des activités criminelles et la sécurité publique.

Par ailleurs, sous l'influence du droit européen, la régulation des traitements de données personnelles a été accrue ces dernières années. Ainsi, le RGPD réaffirme et accentue les droits dévolus aux citoyens européens pour leur garantir une meilleure maîtrise de leurs données personnelles (I). Il se montre également plus sévère envers les responsables de traitement en accentuant les nombreuses obligations qui leurs ont été imposées par les dispositions « informatique et libertés » et étend leur responsabilité dans certains cas de figure (II).

On peut alors noter que le non-respect des droits des individus et des obligations imposées aux responsables de traitement fait l'objet d'une répression pénale « unifiée » depuis la loi du 6 août 2004 transposant les dispositions de la directive de 1995. Celle-ci a rehaussé l'ensemble des peines, qui peuvent désormais aller jusqu'à 300.000€ d'amende et 5 ans d'emprisonnement. Le montant de l'amende encourue peut aller jusqu'à 1.500.000€ lorsque le responsable de traitement est une personne morale, conformément à l'article 226-24 du Code pénal. Il risque également la fermeture de ses établissements. De plus, des peines complémentaires peuvent être prononcées. Il peut ainsi être procédé à la confiscation des appareils nécessaires au traitement ou à la publication de la condamnation, conformément à l'article 226-22-2 du Code pénal. Le responsable de traitement peut également être contraint à l'effacement de données enregistrées sur le fondement de l'article 226-31 du Code pénal. Aux vues de l'énorme valorisation qui peut être faite des données personnelles, cette sanction peut représenter des pertes considérables pour un opérateur numérique, surtout pour celui dont les données représentent la principale source de revenu.

Les sanctions pénales sont à appréhender de manière indépendantes : elles ne sont pas basées sur les dispositions « informatique et liberté » mais sur la sanction d'un manquement à une obligation ou à une interdiction légale. Il peut alors arriver qu'un même manquement fasse l'objet de deux sanctions : une administrative et une pénale, ceci au détriment du principe « non bis in idem » signifiant que des mêmes faits ne peuvent pas être sanctionnés à plusieurs reprises. Mais à ces sanctions pénales se sont substituées, en pratique et la plupart du temps, les sanctions administratives infligées par la CNIL.

I. La réaffirmation et l'évolution des principes relatifs à la protection de la personne.

La régulation « informatique et libertés » créé un certain nombre de droits garantissant aux individus une plus grande maîtrise de leurs données personnelles et une meilleure protection face aux traitements qui peuvent en être faits. Ces droits ont été réaffirmés dans le règlement du 27 avril 2016 (§1). Mais ils sont également amenés à être précisés et renforcés au fil du temps. Des évolutions notables sont ainsi apparues sous l'influence du droit européen (§2).

§1. La réaffirmation des droits accordés aux individus par la législation « informatique et libertés ».

Ces droits, portés par le droit européen et reconduits dans les systèmes juridiques des Etats membres de l'Union européenne visent à donner aux individus les moyens de se protéger contre tout abus qui pourrait être fait de leurs données personnelles. Ce sont des droits qu'il leur appartient d'exercer et qui donnent lieu à une action positive de la part du responsable de traitement. On peut ainsi retrouver le droit à l'information, traduisant la volonté de créer une certaine transparence dans le traitement des données personnelles (A). On retrouve également les droits d'accès (B), de rectification, de mise-à-jour et d'effacement (C) ainsi que le droit dit « d'opposition » (D).

A. Le droit à l'information de la personne concernée : la recherche de transparence dans le traitement des données à caractère personnel.

L'article 32-I de la loi « Informatique et libertés » oblige le responsable de traitement à fournir certaines informations lorsqu'il procède à la collecte de données personnelles. Il doit ainsi informer la personne concernée de son identité, de la finalité du traitement, du caractère facultatif ou obligatoire de sa réponse, des conséquences éventuelles en cas de défaut de réponse. Il doit également lui faire part de l'existence des droits lui étant reconnus, de l'identité du/des destinataire(s) des données, ainsi que l'existence d'éventuels transferts des données vers d'autres Etats.

Le même article limite le droit d'information des personnes concernées dans certains cas. Ainsi, le responsable de traitement n'a pas besoin de les informer lorsque les données sont rendues anonymes. Les seules informations devant être communiquées dans ce cas précis sont l'identité du responsable du traitement et la finalité poursuivie par le traitement. D'autre part, l'information des personnes concernées n'est pas obligatoire lorsque le traitement vise des finalités historiques, statistiques ou scientifiques. Le droit à l'information est également supprimé lorsque les données ont été collectées de manière indirecte et concernent un traitement mis en œuvre pour le compte de l'Etat (sûreté, défense, sécurité publique, exécution d'une condamnation pénale). La limitation du droit d'information doit cependant être nécessaire au but poursuivi. Enfin, lorsque l'information des personnes concernées est impossible ou lorsqu'elle exige des « efforts disproportionnés », le responsable de traitement peut en être déchargé. Il devra alors démontrer au juge où à la CNIL que l'information de la personne concernée exigeait de lui des efforts réellement « disproportionnés ».

Le non-respect du droit d'information expose le responsable de traitement aux dispositions de l'article R. 625-10 du Code pénal qui reprend la formulation de l'article 32 la loi « Informatique et libertés ». Il s'agit d'une contravention de 5ème classe. Cependant, on peut se poser la question de la teneur du consentement d'un individu à la collecte de ses données personnelles lorsqu'il n'a pas été informé des modalités du traitement envisagé. En effet, dans de pareilles circonstances, le consentement donné est-il bien libre et éclairé ? Alors, l'absence d'information de la personne concernée ne serait-elle pas assimilable à une absence de consentement qui, comme nous le verrons plus tard, est sanctionnée de manière beaucoup plus rigoureuse.

B. Le droits d'accès accompagnant la logique de transparence du traitement de données à caractère personnel.

L'article 39 de la loi « Informatique et libertés » donne à la personne concernée par la collecte ou le traitement de données personnelles la possibilité d'interroger le responsable du traitement. Elle peut demander à prendre connaissance de l'ensemble des données que celui-ci détient sur elle. Cette demande n'a pas besoin d'être justifiée. La personne concernée doit alors obtenir : la confirmation que des données la concernant font ou non l'objet d'un traitement ; des informations sur l'origine de ces données ; des informations sur la finalité du traitement mis en œuvre, la catégorie des données concernées et leur destinataire potentiel ; ainsi que la communication des données. Le droit d'accès doit être direct, personnel (le demandeur devra à

ce titre fournir un document attestant de son identité),[38] discrétionnaire et permanent. Cependant, la communication de la copie des données et des informations afférentes peut être mise à la charge de la personne concernée. La demande ne doit pas être abusive, sinon le responsable du traitement peut s'y opposer sur le fondement de l'article 39-II de la loi « Informatique et libertés ». L'abus peut notamment se manifester dans le cas de demandes répétées ou systématiques. Le non-respect du droit d'accès par le responsable de traitement l'expose à une contravention de 5ème classe, conformément à l'article R. 625-11 du Code pénal.

C. *Le droit de rectification, de mise-à-jour et d'effacement assurant à l'individu la maîtrise de ses données personnelles.*

L'article 40 de la loi « Informatique et libertés » prévoit la possibilité pour toute personne concernée de demander au responsable de traitement de rectifier, compléter, mettre à jour, verrouiller ou supprimer des données la concernant si celles-ci sont incomplètes, inexactes, équivoques, obsolètes ou si leur collecte ou conservation est interdite. Cette demande doit pouvoir être exercée de manière gratuite. Lorsque le responsable du traitement prend connaissance de l'exercice par un individu de son droit de rectification ou d'effacement, il doit en informer les tiers à qui il a pu communiquer les données. Dans le cadre d'une telle demande, le responsable du traitement doit justifier, à ses propres frais, qu'il a bien été procédé aux modifications ou à la suppression qui lui ont été demandées. Le non-respect de ces droits expose, là encore, le responsable de traitement à une contravention de 5ème classe, conformément à l'article R. 625-12 CP.

Les droits de rectification et d'effacement font l'objet d'une application particulière pour les hébergeurs. L'hébergeur est, au sens de la loi « LCEN » celui « *qui assure, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».[39] L'hébergeur est soumis à un régime particulier : celui de la responsabilité limitée.

[38] *Article 92 du décret 2005-1309 du 20 octobre 2005*

[39] *Article 6-1-2 de la loi n° 2004-575 pour la confiance dans l'économie numérique*

En effet, il n'est pas considéré comme responsable des contenus qu'il héberge mais comme un simple intermédiaire entre le réseau et l'éditeur du contenu. Il n'a donc aucune obligation légale de contrôler les informations qu'il fait simplement transiter. Il serait surement excessif, en termes de ressources, d'exiger de l'hébergeur qu'il s'assure de la licéité, de la véracité ou de la pertinence de l'information avant de la relayer. Ce serait également donner à l'hébergeur un rôle de censeur qui ne lui incombe pas et qui s'opposerait à une des clés de voûte de l'Internet : la liberté d'expression. Ce régime trouve à s'appliquer tant que l'hébergeur n'a pas connaissance du caractère illicite des informations. En effet, dès lors qu'il en prend connaissance, il devient responsable s'il ne procède pas rapidement à la suppression du contenu. L'illicéité peut apparaître à l'hébergeur de manière spontanée (vente de drogue, d'arme, documents pédopornographiques, etc.), ou être décidée par un juge. Dans ce cas, l'hébergeur attendra la communication de la décision de Justice pour procéder à l'effacement.

Toutefois, il a pu être jugé en première instance qu'en matière de protection des données personnelles, l'hébergeur ne peut se prévaloir de son statut d'intermédiaire et du régime de responsabilité limitée qu'il sous-entend. En effet, le juge a estimé que l'hébergeur était tenu d'effacer des données personnelles dès lors que cela lui était demandé par la personne concernée, que les données soient ou non illicites. Il devient alors responsable des données personnelles qu'il véhicule lorsqu'il refuse de procéder à leur suppression, requise par la personne concernée pour des « motifs légitimes » (comme une atteinte à sa vie privée). Il pourra ainsi être amené à lui reverser une indemnisation. Mais cette jurisprudence reste marginale et ne suffit pas, en l'absence de dispositions contraires, à écarter la responsabilité limitée de l'hébergeur de contenu numérique.[40]

D. Le droit d'opposition : maîtrise ultime donnée à l'individu sur ses données personnelles ?

L'article 38 de la loi « Informatique et libertés » reconnaît à toute personne la possibilité de s'opposer à ce que ses données fassent l'objet d'un traitement. Cette possibilité est appelée « droit à l'oubli » par le RGPD. Le droit d'opposition ne doit pas être confondu avec le droit d'effacement ou de rectification. En effet, il s'agit là d'un droit global. Ainsi, il ne se limite pas aux données inexactes, périmées, ou dont le traitement est interdit mais s'applique à l'ensemble

[40] *CA Montpellier, 15 décembre 2011*

du processus de traitement et peut être soulevé à n'importe quel stade de celui-ci, que cela concerne la donnée de manière spécifique ou le traitement lui-même.

Il peut s'appliquer à la totalité des données qui peuvent être recueillies sur une personne. Mais il n'est pas pour autant absolu. En effet, ce droit s'oppose à des intérêts collectifs comme la liberté d'expression ou la liberté d'information. Le demandeur doit alors démontrer la présence d'un « motif légitime » justifiant sa demande, hormis dans l'hypothèse où le traitement serait réalisé à des fins commerciales ou de profilage politique, religieux, syndical, etc. Dans ce cas, le droit d'opposition est acquis « par défaut » par la personne concernée. En effet, en matière de données sensibles, « *la légitimité de l'opposition est remplie par le seul exercice de la faculté d'opposition* ».[41]

Ainsi, dans la pratique, l'application de ce droit d'opposition a eu l'occasion de se confronter à d'autres impératifs d'intérêt général comme la liberté d'expression ou le droit à l'information. Il s'est parfois incliné[42] et s'est d'autre fois vu affirmé par des magistrats, faisant pencher la balance en faveur du droit au respect de la vie privée et au respect de l'intégrité.[43]

Le non-respect du droit d'opposition est assimilé à une collecte déloyale, sanctionné par l'article 226-18-1 du Code pénal. Par ailleurs, la méconnaissance du droit d'opposition en matière de recherche médicale fait l'objet d'un article distinct : l'article 226-19-1 du Code pénal. Toutefois, le droit d'opposition n'existe pas pour certains fichiers de l'administration (Police, Justice, services fiscaux, sécurité sociale, etc.). Il n'a pas non plus vocation à s'appliquer lorsque le traitement est soumis à une obligation légale comme par exemple le fichier d'état civil, contrairement au fichier de recensement - dit « de population » - qui lui, n'est pas obligatoire. Dans le cas d'un fichier administratif facultatif, l'administré doit être informé qu'il peut refuser la collecte de données le concernant.[44]

---

[41] Cass. Crim., 28 septembre 2004, n° 03-86.604 « Association spirituelle de l'église de scientologie de l'Île-de-France »

[42] Voir par exemple : Cass. 1ère civ., 20 novembre 1990 ; CA Aix-en-Provence, 24 octobre 2006

[43] Voir par exemple : TGI Paris, 15 février 2012, Diana Z. c/ Google concernant une ancienne actrice qui demandait la suppression de la connexité entre son nom et des vidéos pornographiques dans lesquelles elle avait tourné

[44] Jérôme Lefort, Marion Hainez et Marine Chatelet, « Gérer, sécuriser et valoriser ses données personnelles des collectivités territoriales », Territorial Editions, 2015, p. 26

§2. : L'influence du droit européen sur les évolutions des droits de la personne.

Les droits reconnus aux citoyens européens ont été récemment renforcés sous l'influence du droit européen. Qu'il s'agisse du « droit au déréférencement » - corolaire du « droit à l'oubli » - créé par le juge européen (C) ou encore de droits portés par le règlement du 27 avril 2016, comme la protection des données personnelles des mineurs (A) ou le droit à la portabilité des données personnelles (B).

A. L'intensification de la protection des données personnelles des mineurs.

L'univers numérique peut se révéler particulièrement dangereux pour les libertés fondamentales des citoyens, a fortiori pour celles des mineurs, dont la capacité de discernement est réduite. En ce qui concerne les services de la « société d'information », c'est-à-dire « *tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* »,[45] le consentement d'un mineur de moins de 16 ans doit être donné par son représentant légal. L'article 8 du RGPD reprend ce principe et fait obligation aux responsables de traitement de recueillir l'autorisation des responsables légaux des mineurs de moins de 16 ans pour procéder à la collecte de données les concernant. Il laisse toutefois une marge d'appréciation aux Etats membres pour déterminer l'âge minimum pour l'application de cette protection spécifique (dans la limite d'un minimum de 13 ans). Par ailleurs, les acteurs du numérique doivent prendre garde à ce que les informations qu'ils donnent sur les conditions de la collecte et les modalités du traitement soient bien intelligibles pour les mineurs : ils doivent utiliser un langage simple ou une iconographie représentative.

B. L'introduction d'un droit à la portabilité des données personnelles ;

La portabilité des données est un droit fondamental dans le cadre de la construction d'un « Marché unique numérique ». Elle est affirmée dans le règlement du 27 avril 2016.

[45] *Article 1er de la Directive n° 98/34/CE du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et règlementations techniques et des règles relatives aux services de la société de l'information*

Le droit à la portabilité a pour origine la régulation des télécoms. Il s'agit du droit à garder son numéro de téléphone lorsque l'on change d'opérateur. Il est l'une des émanations de la liberté de circulation. Dans l'Union européenne, les éléments liés à la personne sont amenés à pouvoir librement traverser les frontières des Etats membres. Il peut s'agir par exemple d'informations comme le nom, le statut marital, la filiation, etc. Toute personne jouira du droit à la portabilité des données qui s'appliquera lorsque le consentement de la personne concernée aura été recueilli, lorsque le traitement sera nécessaire à l'exécution d'un contrat, ou encore dès lors que le traitement sera effectué à l'aide de procédés automatisés.

Ainsi, les personnes concernées auront le droit de se faire communiquer les données personnelles qu'un responsable de traitement détient sur elles et de les transmettre librement à un nouvel opérateur. Cette transmission devra, lorsque cela sera techniquement possible, être réalisée de manière directe, entre les responsables de traitement.

C. *L'introduction par le juge européen d'un droit au déréférencement sur l'Internet.*

Le droit au déréférencement est l'émanation du « droit à l'oubli » sur l'Internet, qui doit s'entendre au sens d'un droit « *offert aux citoyens de conserver dans le temps la maîtrise de leurs données personnelles, afin notamment d'obtenir leur suppression ou leur effacement quand ils le souhaitent* »[46]. Sa création découle de l'arrêt « Google Spain ».[47] Mais il faut souligner les problématiques qu'il engendre (1). Il s'agira alors d'en étudier la mise en œuvre chez l'opérateur majeur du secteur : la société Google (2).

1) *Les problématiques soulevées par le droit au déréférencement.*

La Cour y a dégagé la possibilité, pour un internaute, de demander à un moteur de recherche de « délier » son identité avec certaines informations le concernant. Le déréférencement est une alternative pragmatique mais insuffisante à la suppression des données sur Internet. Pragmatique, car il est en pratique impossible de supprimer totalement des données personnelles mises en ligne. Insuffisante, car même déréférencées, les données demeurent sur

[46] *Rapport annuel du Conseil d'Etat (2014) publié le 9 septembre 2014, Recommandation n° 5*

[47] *Arrêt CJUE, 13 mai 2014, n° C 131/12, dit « Google Spain »*

le web et peuvent être captées par quiconque arrive à les retrouver, tâche ardue pour un être humain mais aisée pour une machine, surtout avec le développement des « métadonnées », agissant comme des balises informatrices accrochée aux données, créant de « l'information sur l'information ».

Cette possibilité est offerte à toute personne dont les informations, mêmes véridiques, ont été recueillies de manière illicite ou présentent un caractère inadéquat, non pertinent ou excessif.[48] En cas de refus de la part du moteur de recherche, le demandeur peut introduire une action devant l'autorité administrative compétente ou une juridiction nationale. La Cour estime par conséquent que, même s'ils n'ont qu'un rôle d'intermédiaire dans le relai de l'information et n'ont pas eux-mêmes participé à la collecte ou à la mise en ligne de l'information, les moteurs de recherche en effectuent un traitement dont ils sont responsables en l'indexant puis en la retranscrivant. Malgré les apparences, le droit au référencement n'est pas un droit nouveau mais une simple application aux moteurs de recherche d'un croisement entre le droit d'effacement et le droit d'opposition. Si elle souhaite la suppression de pages web, la personne concernée doit alors exercer ses droits à l'encontre du responsable du traitement initial ayant publié l'information sur Internet.

En l'absence de directions précises données par le juge européen, les moteurs de recherche doivent mettre en place une politique interne pour gérer les demandes et fixer eux-mêmes les critères du déréférencement. En dehors des cas évidents (victimes de crimes, de viol, d'abus sur les réseaux sociaux, etc.), les juristes du moteur de recherche devront eux-mêmes assurer l'application du droit national. S'ils n'y parviennent pas, ils laissent le contenu sur le réseau et invitent la personne concernée à saisir les tribunaux. Il leur faut donc prendre en compte la nature du site web, la qualité de la personne en cause (pas simplement si la personne est publique ou non) ainsi que la nature des informations. C'est alors le moteur de recherche qui va devoir opérer la balance entre les intérêts et les libertés fondamentales en présence : liberté d'expression et droit à l'information, d'un côté et droit au respect de la vie privée, de l'autre. Or, comme le rappelle le Conseil d'Etat[49], c'est aux autorités judiciaires de mesurer les intérêts en présence et d'en assurer le juste équilibre, conformément à l'article 66 de la Constitution.

---

[48] Voir : Ordonnance de référé, TGI Paris, 19 décembre 2014 pour une condamnation pénale datant de plus de 8 ans qui ne figurait pas sur le casier judiciaire du demandeur

[49] Recommandation n° 5, Rapport annuel du Conseil d'Etat (2014) publié le 9 septembre 2014

Ainsi, la haute juridiction administrative conseille de réintroduire une intervention judiciaire dans le processus de déréférencement. L'éditeur du contenu faisant l'objet de la demande de déréférencement devrait pouvoir faire valoir ses observations au moteur de recherche et saisir le juge en cas de désaccord. Le Conseil d'Etat invite également à l'introduction des autorités nationales dans ce processus. Enfin, pour éviter que le déréférencement ne soit exécuté que par le seul moteur de recherche à qui il a été demandé, le Conseil d'Etat propose des solutions pour qu'une décision « unique » puisse être rendue. Il prévoit trois possibilités. Tout d'abord, la mise en place d'un système de reconnaissance mutuelle des décisions, ce qui ne semble pas évident car il s'agit d'une décision subjective qui peut fluctuer en fonction de la culture, de la nationalité, de la conception de la liberté d'expression, etc. Effectivement, les moteurs de recherche, bien que principalement américains, n'ont pas tous les mêmes philosophies. D'autre part, le Conseil d'Etat invite à la création d'une instance décisionnelle commune aux moteurs de recherche. Ils lui délégueraient alors leurs capacités de décision. Cette solution peut paraître plus raisonnable mais ne doterait pas la décision d'une plus grande légitimité. Enfin, le Conseil d'Etat préconise la création d'un dispositif légal permettant d'étendre une décision prise par un opérateur à tous ses concurrents, sous réserve de son homologation par un juge.

2) La mise en œuvre du droit au déréférencement par l'entreprise Google.

En tant que premier moteur de recherche européen, Google est touché de plein fouet par cette création prétorienne. En effet, seulement un an après l'arrêt « Google Spain », l'entreprise avait déjà reçu environ 350.000 demandes, dont près de 75.000 en France. La moitié des demandes de déréférencement ont été acceptées en France, contre 40 % dans le reste de l'Europe. Sur l'ensemble des analyses de pages web réalisées, Google n'a eu qu'une dizaine de contentieux (7 en référés, 3 au fond). Le moteur de recherche a dû mettre en place une politique interne en matière de droit au déréférencement. Ainsi, si la demande concerne un contenu journalistique, Google choisit de ne pas l'accepter, même si le juge européen l'a invité à le faire en présence d'articles de presse. Il fait le choix de ne pas retirer le contenu car il serait trop simple de contourner le droit de la presse (nécessité de la qualification d'une diffamation, prescription, etc.). De la même manière, si les informations touchent un homme politique, Google choisit également de ne pas les déréférencer.[50]

[50] *Intervention de Maria Gomri, directrice du service juridique de Google France au Colloque IRDEIC CDA : « L'impact des grands arrêts de la CJUE relatifs aux données personnelles », 5 février 2016*

Google a par exemple refusé de déréférencer un article sur le procès d'un homme d'affaires polonais ; un article sur une ancienne condamnation criminelle d'un homme politique hongrois ; un autre sur la condamnation d'un prêtre français pour détention d'images pédophiles ; un relatif à l'arrestation d'un financier italien. Par contre, le moteur de recherche a accepté des demandes concernant un article sur la condamnation d'une personne en première instance (la personne ayant gagné en appel) ; des pages révélant l'adresse du domicile d'une personne en Suède ; ou encore une page reprenant une photographie personnelle sans l'accord de la personne concernée.[51]

Il faut préciser qu'en cas d'acceptation de la demande de déréférencement, Google n'y procède que sur ses extensions européennes. Le déréférencement est donc limité puisque le contenu reste accessible sur les autres extensions. La CNIL a alors mis Google en demeure d'appliquer le déréférencement à la totalité de ses extensions.[52] Cette position marginale est adoptée par la seule CNIL française, ces homologues européennes se satisfaisant des déréférencements sur les seuls noms de domaines européens. En effet, 97% des utilisateurs européens font leurs recherches sur une extension européenne. Un nouveau bras de fer s'est alors engagé entre la CNIL et Google, qui refuse de s'y résoudre. En effet, le moteur de recherche estime que le droit européen et plus particulièrement les décisions de la CJUE, n'ont vocation à s'appliquer que sur le territoire européen. L'entreprise estime également qu'imposer un déréférencement dans d'autres Etats reviendrait à pratiquer une sorte d'ingérence. Elle indique qu'il faudrait alors appliquer, sur le sol européen, des décisions provenant d'autres pays qui n'auraient pas forcément la même manière d'appréhender la liberté d'expression. Cela reviendrait donc à appauvrir le contenu du web de manière négative, à la réduire au plus petit dénominateur commun.

[51] *Compte rendu des déréférencements opérés par Google (2015). Voir : www.google.com/transparencyreport/removals/europeprivacy/hl=en30/7/2015*

[52] *Décision CNIL n° 2015-047 du 21 mai 2015*

II. L’extension de la régulation des pratiques du responsable de traitement.

En plus des droits dévolus aux individus, la régulation du traitement des données personnelles nécessite que le processus de traitement lui-même soit encadré par des principes forts. Des obligations et des interdictions doivent donc être respectées par les responsables de traitement (§1). Par ailleurs, pour assurer une protection toujours plus rigoureuse des libertés fondamentales des citoyens européens, la responsabilité des opérateurs procédant au traitement des données personnelles a été étendue sous l’influence du droit européen (§2).

§1. L’évolution des obligations imposées au responsable de traitement.

La collecte de données est la première étape du mécanisme de traitement. C’est une phase importante qui se doit d’être encadrée aussi rigoureusement que ne l’est le traitement. La collecte doit ainsi être limitée par le respect de la vie privée des personnes concernées. La législation « informatique et libertés » prévoit donc des conditions de régularité pour la collecte de données personnelles elle-même (A), tandis que d’autres ont vocation à perdurer durant l’ensemble de la durée de vie des données (B). Ces conditions de régularité se matérialisent sous la forme d’obligations mises à la charge du responsable de traitement.

A. Les restrictions propres à la collecte de données personnelles.

Aux vues de l’importance de la collecte de données dans le processus de traitement, les dispositions législatives l’encadrant se multiplient. Il s’agit d’éviter que la collecte ne soit réalisée sans aucune limite. Ainsi, la collecte doit être encadrée par la détermination de la finalité du traitement envisagé (4) et doit être proportionnée à l’objectif recherché (5). D’autre part, les données personnelles ne peuvent être recueillies de manière déloyale, illicite ou trompeuse (1) ou en l’absence de consentement des personnes concernées (2). Enfin, la collecte de données dites « sensibles » est rigoureusement encadrée en raison des risques qui peuvent en résulter pour les libertés fondamentales des individus (3).

1) Le principe de loyauté et de licéité de la collecte, ou « principe de transparence ».

L'article 6 de la loi « Informatique et libertés » oblige le responsable de traitement à assurer l'information de la personne concernée lors de la collecte de ses données personnelles. Ainsi, la collecte ne doit pas être réalisée à l'insu de la personne concernée.

La collecte de données personnelles par un moyen déloyal, illicite ou frauduleux expose le responsable de traitement aux dispositions de l'article 226-18 du Code pénal. On peut trouver certaines redondances dans la rédaction de l'article : « déloyal », « illicite », « moyen frauduleux ». Cela offre une plus grande marge d'appréciation au juge. Cette rédaction peut laisser penser que l'incrimination portée est extrêmement étendue en ce sens qu'elle permettrait de s'opposer à des infractions à la loi « Informatique et libertés ». Par exemple, en cas de sollicitations commerciales (« Spam »), cet article permettrait de porter plainte contre l'émetteur puisque l'adresse mail aurait été collectée sans l'accord du destinataire ou de manière frauduleuse (piratage d'une base de données). De la même manière, en cas de non-respect des formalités préalables au traitement, les données seraient également collectées de manière illicite, en l'absence de déclaration ou d'autorisation de la CNIL. Pourtant, le Code pénal prévoit de nombreuses infractions, plus spécifiques, lorsque le traitement lui-même est susceptible de méconnaitre les dispositions et principes posés par la loi « Informatique et libertés ».

Le recours à l'article 226-18 du Code pénal doit donc être vu comme un socle, un fondement général à l'action en justice. Il est complété par la possibilité de recourir à de nombreuses autres infractions prévues par le Code pénal. C'est donc une sorte de moyen de sécurité général, garantissant à l'individu un recours « standard » lorsque ses libertés fondamentales se retrouveraient bafouées lors de leur collecte ou de leur manipulation.

2) L'obligation de recueillir le consentement de la personne concernée.

L'article 7 de la loi « Informatique et libertés » porte l'obligation pour le responsable de traitement de recueillir le consentement de la personne concernée avant de procéder à la collecte de ses données personnelles. Le consentement recueilli doit être éclairé et exprimé en toute connaissance de cause : l'individu doit être au fait de l'existence, des modalités et des finalités du traitement qui sera opéré.

Des exceptions au recueil du consentement existent lorsque le traitement envisagé est nécessaire à l'intérêt vital de la personne concernée ; lorsqu'il répond à une obligation légale ou à une mission de service public ; ou encore lorsque le traitement est nécessaire à la réalisation d'un intérêt légitime du responsable de traitement. Pour ce qui est du démarchage commercial, le consentement doit être recueilli pour toute prospection automatisée sous forme de mails. Sauf pour des personnes qui sont déjà clientes et lorsqu'il s'agit de leur proposer des produits ou services équivalents. Dans ce cas, le client doit avoir la possibilité de faire cesser le démarchage. Cela s'exprime, en pratique, par la possibilité de se désabonner aux sollicitations commerciales. L'exercice de cette faculté doit être simple. Souvent, il s'agit d'un lien se trouvant à la fin du mail reçu et sur lequel cliquer.

Comment prouver que le consentement « indubitable » a bien été recueilli ? Comment être sûr que c'est bien la personne concernée qui a reçu l'information ou qui a exprimé sa volonté ? Ces problématiques se retrouvent principalement sur l'Internet où la personne concernée n'a aucun contact physique avec le responsable de traitement. L'usage de « cookies » en est un très bon exemple. Le terme de « cookie » désigne un fichier stocké dans la mémoire de l'équipement de l'utilisateur. Les cookies sont déposés par le serveur du service consulté et contiennent des informations sur la navigation. Ils vont ainsi permette de conserver une trace du passage de l'utilisateur sur une page web. Ils peuvent par exemple servir à enregistrer les préférences d'un internaute. Certains cookies peuvent être utilisés pour mettre en œuvre un dispositif de publicité ou d'offres commerciales ciblées. D'autres sont nécessaires à la navigation et sont d'ordre purement technique (par exemple, « cookies HTTP » ou « cookies flash »). Si les cookies offrent des opportunités économiques aux opérateurs commerciaux, ils représentent par contre un risque pour la vie privée des internautes.

Les Directives du 25 novembre 2009 formant le « Paquet télécom » régulent l'utilisation des « cookies » par les prestataires de services sur Internet pour espionner ou suivre la navigation de l'utilisateur. Celui-ci doit alors avoir donné son autorisation, après avoir reçu une information claire et précise sur les finalités du traitement. Pour recueillir le consentement, deux techniques s'offrent à l'opérateur : l' « opt-out », qui suppose le consentement par défaut mais la possibilité de résilier l'accord tacite à tout moment ; et l' « opt-in », qui consiste à cocher une case pour montrer son acceptation de manière explicite.

L' « opt in » est la règle en matière de prospection commerciale depuis la Directive « vie privée et communications électroniques »[53]. Obliger les opérateurs à donner une information précise sur chaque traitement a conduit à généraliser la pratique de l' « opt-in » pour les fournisseurs d'accès (FAI) et les opérateurs téléphoniques. Mais il s'agit en réalité d'un « opt-in » aménagé, qui passe par les réglages du navigateur de l'utilisateur. En effet, celui-ci peut configurer les options de navigation pour, soit accepter les cookies de manière générale, soit demander à prendre connaissance de chaque cookie pour choisir lesquels il va accepter et lesquels il va refuser.

Face à une grande disparité dans l'application des dispositions du « Paquet télécoms » concernant l'usage des cookies, la CNIL a rédigé une recommandation.[54] Elle invite les opérateurs du numérique à assurer une information « *visible, mise en évidence et complète* » de l'utilisateur. Pour assurer cette information, les opérateurs doivent avoir recours à des termes simples et compréhensibles par tous et éclairer l'internaute sur l'ensemble des finalités des cookies. La CNIL recommande ainsi le recours à un bandeau d'information apparaissant dès l'entrée sur le site web et regroupant toutes les informations nécessaires (finalités, possibilité de s'opposer, de modifier ses paramètres). L'acceptation de l'internaute sera manifestée par la poursuite de la navigation, le bandeau devant donc être maintenu jusqu'à ce que l'internaute change de page. En ce qui concerne les applications, qui ne passent pas par un navigateur web et dont les cookies sont directement stockés sur l'appareil de l'utilisateur, la CNIL indique que le consentement doit être demandé au démarrage et redemandé de manière régulière. Il ne peut donc s'exprimer par le seul consentement aux conditions générales d'utilisation (CGU) lors de la première utilisation de l'application, comme cela a pu être le cas à de très nombreuses reprises. D'autre part, la CNIL recommande de limiter la durée de stockage des cookies sur l'équipement de l'usager à treize mois, au-delà desquels le consentement devra être redemandé.

3) L'interdiction de traitement des données sensibles.

Le traitement de certaines données est, en principe, interdit en raison du risque qu'elles représentent pour les libertés fondamentales de la personne à laquelle elles se rattachent. Il s'agit de données dites « sensibles ».

---

[53] *Directive 2002/58/CE 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*

[54] *Recommandation CNIL du 5 décembre 2013 n° 2013-378*

L'article 8 de la loi « Informatique et libertés » indique ainsi qu' « *il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». Il peut également s'agir de données comprenant le « numéro de sécurité sociale » (NIR) d'une personne ; de données comportant des appréciations sur les difficultés sociales d'une personne[55] ; ou encore de données biométriques nécessaires à l'identification d'un individu. En ce qui concerne le NIR, la loi est très prévoyante car l'interconnexion de traitements comportant ce numéro pourrait permettre le ré-identification et l'accès à de nombreux aspects de la vie privée de l'individu. Il s'agit cependant d'une disposition purement française. En effet, dans d'autres Etats de l'Union, un numéro similaire au NIR est utilisé comme identifiant des personnes sans que cela ne porte atteinte à leurs libertés. Ces divergences expliquent la prudence affichée par le RGPD en la matière. En effet, son article 87 permet aux Etats membres de « *prévoir des dispositions plus précises pour les numéros nationaux d'identification* ». Afin de promouvoir la recherche publique, le Projet de loi « pour une République numérique » propose d'utiliser un numéro dérivé du NIR et d'en faciliter l'utilisation par les organismes de traitement.

De la même manière, l'article 9 de la loi « Informatique et libertés » encadre la collecte de données concernant les infractions et les condamnations pénales. Ces données ne peuvent être manipulées que par les juridictions, les autorités publiques et les établissements chargés d'une mission de service public qui agissent dans le cadre de leurs attributions légales.

Le non-respect de l'encadrement de la collecte de données sensibles fait l'objet des articles 226-19 et 226-23 du Code pénal. Une infraction spécifique a été rajoutée à l'article 226-16-1 du Code pénal par la loi du 6 août 2004 transposant la directive de 1995. Elle concerne les données personnelles ayant à trait au NIR des personnes concernées.

La loi aménage quelques exceptions autorisant le traitement de ces données, souvent en présence d'un autre intérêt « supérieur » aux risques encourus par la personne concernée. C'est également le cas lorsque les données ont été rendues publiques par cette personne ou lorsqu'elle

[55] *Article 25-I, alinéa 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

en a accepté la collecte. Deux d'entre elles sont à mettre en avant en raison de l'ampleur de leur occurrence dans la pratique. Premièrement, la loi autorise le traitement de données sensibles divulguées par la personne concernée elle-même.[56] C'est ici tout l'enjeu et la contrepartie de la gratuité apparente dont se targuent de plus en plus de prestataires de services sur le web et, plus particulièrement, les réseaux sociaux (dont la principale source de revenus se trouve dans la valorisation des données personnelles de leurs utilisateurs). C'est pourquoi ces derniers permettent et incitent leurs utilisateurs à donner le plus de renseignements possibles sur eux-mêmes, que ce soit dans une logique consumériste, ou dans une logique encore plus intimiste (orientations religieuses, politiques, sexuelles, etc.). Un manque de conscience de la relativité de cette « fausse gratuité » peut aboutir à la perte par les individus de la maîtrise de leurs données personnelles. Ensuite, la loi a aménagé l'interdiction du traitement de données sensibles en la conciliant avec la liberté d'expression et, plus précisément, avec le droit de la presse. C'est ainsi que l'article 37 de la loi « Informatique et libertés » instaure une dérogation à de tels traitements dans le cadre de la mission d'information qui incombe au journaliste. Cette dérogation est toutefois cloisonnée au respect de la déontologie professionnelle, celle-ci obéissant aux dispositions des Codes civil, pénal et de la Loi du 29 juillet 1881, dite « Loi de la Presse ». Ainsi, des informations sur des affaires judiciaires en cours peuvent être relayées par des sociétés de presse, bien qu'ayant recours à l'utilisation de données personnelles.[57]

Enfin, il faut indiquer que le RGPD opère un changement dans la dénomination des données sensibles qui seront désormais appelées « catégories particulières ».

4) Le principe de finalité de la collecte.

L'article 6, alinéa 2 de la loi « Informatique et libertés » prévoit le principe de finalité. Celui-ci consiste à déterminer la finalité du traitement envisagé. Les données ne pourront pas, par la suite, être utilisées dans d'autres objectifs. Cette obligation imposée au responsable de traitement permet de limiter la collecte. La finalité doit être déterminée de manière explicite, c'est-à-dire qu'elle doit être claire, précise et sans équivoque. Le G-29 a par ailleurs indiqué qu'elle devait être exprimée de manière intelligible par tous, quelle que soit la langue ou la culture de la personne concernée. Elle doit également être légitime. Cela signifie qu'elle ne doit

[56] *Article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

[57] *Voir par exemple : TGI Paris, 17ème chambre correctionnelle, 6 juin 2001*

pas heurter les libertés fondamentales des personnes concernées. En cas de modification ou d'élargissement de la finalité déterminée initialement, la CNIL doit être informée par le responsable du traitement. Celui-ci devra également accomplir de nouveau, le cas échéant, les formalités nécessaires.

Des exceptions au principe de finalité sont prévues à l'article 36 de la loi « Informatique et libertés ». Ainsi, les données peuvent être réutilisées au cours d'un traitement poursuivant un objectif autre que celui prévu lors de leur collecte lorsque la personne concernée a manifesté son consentement ou lorsque la CNIL a donné son autorisation. Dans le cas où ces données seraient sensibles, elles peuvent faire l'objet d'un traitement ultérieur dont la finalité aurait été modifiée dans le cadre de la recherche dans le domaine de la santé, ou encore lorsque l'intérêt public le justifie. Une dérogation est également apportée au principe de finalité par le RGPD. Si elle concerne la collecte et le traitement de masses de données (« Big Data »), elle reste assez similaire à ce que prévoit la législation actuelle. Ainsi, la réutilisation ultérieure des données est possible si elle obtient le consentement des personnes concernées, si elle est permise par une loi, nécessaire à la réalisation d'un contrat, etc. Dans le cas où les nouvelles finalités diffèreraient de celles qui ont été déterminées initialement, il faudra alors prendre en compte les mesures de protection engagées par le responsable du traitement (pseudonymisation ou cryptage des données).

La finalité déterminée ne se limite pas à la collecte et s'étend également à l'usage qui pourra être fait des données par la suite. Les données ne peuvent donc pas être réutilisées pour un autre but que la finalité déterminée lors de la collecte. Ainsi, le principe de finalité évite l'usage malveillant ou détourné des données.

5) Le principe de proportionnalité de la collecte.

L'article 6, alinéa 3 de la loi « Informatique et libertés », introduit par la loi de du 6 août 2004 transposant la directive de 1995, indique que les données doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ». Le législateur a intégré un principe de proportionnalité encadrant la collecte des données personnelles. Celle-ci est alors limitée aux seules données « pertinentes » en vue de l'objectif défini initialement par le responsable du traitement. Il ne peut donc collecter des données à tout va.

B. *Les restrictions perdurant durant la totalité de la durée de vie des données personnelles.*

En plus de l'encadrement de la collecte des données personnelles, des obligations couvrant la totalité de leur durée de vie sont imposées au responsable de traitement. Il s'agit alors du respect du « principe de temporalité », limitant la durée de conservation des données par le responsable de traitement (1). Ce dernier doit également assurer la sécurité et la confidentialité des données qu'il stocke (2) et procéder à des notifications lorsque celles-ci seraient compromises (3). Le champ d'application de cette dernière obligation est étendu par le règlement du 27 avril 2016.

1) *Le principe de conservation limitée des données personnelles ou « principe de temporalité ».*

L'article 6, alinéa 5 de la loi « Informatique et libertés » indique que la conservation des données ne peut outrepasser la « *durée prévue par la loi* ». Ainsi, celle-ci doit être adaptée à la finalité recherchée. Mais la loi ne donne aucune indication précise sur cette durée. C'est au responsable du traitement d'estimer la durée de conservation nécessaire en fonction du traitement mis en œuvre et des objectifs poursuivis. La durée de conservation peut donc varier en fonction de la finalité du fichier. On utilise ici souvent la notion de « droit à l'oubli », qui n'existe pas en tant que telle dans la loi. En réalité, l'obligation de supprimer les données personnelles au-delà d'un certain temps est un des prémices du « droit à l'oubli » numérique. On peut d'ailleurs se poser quelques questions sur l'effectivité d'un tel droit. En effet, l'effacement d'une donnée revient souvent, en pratique, à l'effacer des « registres » et non en sa suppression matérielle. Elle reste donc bien présente sur un support physique et l'on peut la récupérer sur un disque dur, une imprimante, etc. De plus, dans le cadre des données mises en ligne, le recours croissant aux caches, aux pages miroirs, etc. réduit considérablement la capacité à supprimer la donnée une fois qu'elle a été diffusée. Le seul fait de détruire le support matériel de la donnée à l'intérieur d'un serveur de stockage ne semble donc plus suffire à ce que celle-ci disparaisse complètement du réseau.

Ce principe permet de réguler le « Big Data » en sa nature même. En effet, comme nous avons pu le voir, l'essence d'un traitement de type « Big Data » passe par la collecte massive et continue de données et ce, sans qu'un traitement ne soit nécessairement défini par avance. Il s'agit donc de collecter des données pour décider plus tard de ce qui en sera fait.

Limiter la conservation des donnés dans le temps permet donc d'empêcher le fait que les données puissent être réutilisées ou revendues, des années après. Couplée à l'exigence d'une finalité déterminée à l'origine du processus de traitement, la limitation de la durée de conservation des données permet de restreindre de manière considérable la possibilité de collecter des données à tout-va.

Mais, là encore, le législateur n'a pas pour objectif d'ôter tout son potentiel économique au traitement de données personnelles. Des exceptions à ce principe ont donc été prévues lorsque le responsable de traitement se trouve en possession de données « neutralisées », c'est-à-dire qui ont perdu leur caractère personnel ou qui ne représentent pas un danger pour les libertés des personnes concernées. Les autres exceptions au principe de finalité sont énumérées par l'article 36 de la loi « Informatique et libertés ». Elles s'appliquent dès lors que les données sont collectées « *en vue d'être traitées à des fins historiques, statistiques ou scientifiques* », que le responsable du traitement a recueilli le consentement de la personne concernée pour étendre la durée de conservation de ses données, ou qu'il a obtenu une autorisation de la CNIL.

2) L'obligation d'assurer la sécurité et la confidentialité des données stockées.

L'article 34 de la loi « Informatique et libertés » pose une obligation générale de sécurité et de confidentialité. À ce titre, « *le responsable de traitement est tenu de prendre toutes les précautions utiles au regard des risques présentés par le traitement pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Se montrer exigeant face à la réalisation de cette obligation permet, en théorie, d'éviter la compromission de données plus ou moins sensibles et les risques que cela induit pour les libertés fondamentales des personnes concernées.

Or, de telles situations se produisent de manière régulière sans que le public ou même les « victimes » n'en aient forcément conscience. On peut illustrer ce genre de situation par un exemple de « fuite » de données à caractère personnel : les coordonnées de près de 112.000 policiers ont été publiées sur Internet et ce, deux semaines après le meurtre d'un couple de policiers dans les Yvelines. Les données étaient issues de la Mutuelle générale de la Police, pourtant habituée aux attaques informatiques. Cependant, l' « attaque » venait cette fois d'un salarié de la mutuelle, donc de l'intérieur de la structure.

L'obligation de sécurité qui pèse sur le responsable du traitement est modulée en fonction du risque planant sur les libertés de la personne concernée, donc de la sensibilité des données recueillies. Plus celles-ci sont sensibles, plus on va attendre de lui la mise en place d'un niveau de sécurité élevé. La sécurité des données s'entend par leur intégrité, leur authenticité et leur disponibilité. Le responsable du traitement a, en quelque sorte, la garde des données qu'il collecte : il doit veiller à ce qu'elles ne soient pas détournées ou endommagées. Il doit alors mettre en place des mesures de protection techniques et spécifiques. Le responsable de traitement doit également assurer la confidentialité des données qu'il conserve. Cela implique une limitation de l'accès aux données recueillies pour éviter leur divulgation à des « tiers non autorisés ». Seuls des tiers habilités doivent être susceptibles d'y accéder.

La sécurité ne doit ainsi pas être assurée qu'à l'égard des personnes extérieures à l'organisme de traitement, mais également en interne, à l'égard de ses collaborateurs. Ainsi, et par exemple, une société a été condamnée pour la simplicité des mots-de-passe de ses salariés et pour le fait qu'ils n'étaient pas modifiés de manière régulière.[58]

Cette obligation est une obligation de moyen. Cela signifie que le responsable de traitement doit prendre toutes les mesures nécessaires pour assurer la sécurité des données ainsi que leur confidentialité. Cependant, la loi ne précise pas quelles sont les mesures qui doivent être appliquées. Il faut alors prendre en compte la sensibilité des données stockées, les risques qui pèsent sur elles, la pratique ou l'état de l'art ainsi que les coûts que représentent les mesures. C'est le juge qui décidera de la pertinence des moyens employés par le responsable du traitement en cas de violation de la sécurité des données. Par une délibération en date du 21 juillet 1981[59] et la publication d'un guide pratique en 2010,[60] la CNIL invite les opérateurs du numérique à mettre en place des mesures de sécurité dans divers domaines comme l'authentification des utilisateurs, la gestion efficace de l'accès pour le personnel (gestion des habilitations et sensibilisation des utilisateurs), la sécurité des postes de travail, le développement informatique, la traçabilité et la gestion des incidents, ou encore l'anonymisation et le chiffrement des données.

---

[58] *Délibération de la formation restreinte de la CNIL n° 2013-139 du 30 mai 2013, SAS Professional Service Consulting, dite « PS Consulting »*

[59] *Délibération n° 81-094 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques*

[60] *Guide : la sécurité des données personnelles, CNIL, éditions 2010*

L'article 226-17 du Code pénal sanctionne le « défaut de sécurité », c'est-à-dire le fait d'opérer un traitement de données personnelles sans mettre en œuvre les obligations légales en matière de sécurité. Mais le texte est imprécis, la notion de sécurité pouvant aussi bien renvoyer à la sécurité juridique qu'à la sécurité matérielle ou physique des données (sécurité des locaux de stockage des données, par exemple). En cas d'attaque de ses systèmes, le responsable de traitement peut donc être à la fois victime du piratage mais également considéré comme fautif. On peut alors noter que l'article 323-1 du Code pénal sanctionne l'accès frauduleux aux systèmes d'une amende de 60.000€ et de deux ans d'emprisonnement. Alors que le responsable de traitement encourt, pour défaut de sécurité, une amende de 300.000€ et 5 ans d'emprisonnement (amende pouvant être portée à 1.500.000€ dans le cas où le responsable de traitement est une personne morale). Il semblerait donc que ce déséquilibre des peines, qui penche nettement en la défaveur du responsable de traitement, ait pour objectif de sensibiliser ces derniers à sécuriser au mieux leurs systèmes. Par ailleurs, l'article 226-17 du Code pénal ne fait pas de distinction entre le responsable de traitement ayant sciemment refusé de mettre en place une protection effective des données personnelles en sa possession et le responsable de traitement simplement négligent. La sanction encourue (5 ans d'emprisonnement) peut alors paraître quelque peu excessive.

3) L'obligation de notifier les failles de sécurité, étendue à tous les responsables de traitement.

L'obligation de notification des failles de sécurité trouve sa source dans le concept américain de « Data breach » qui oblige la victime d'une cyberattaque à se manifester et à faire preuve de transparence de manière à mieux pouvoir en appréhender l'auteur. En Europe, cette obligation est portée par le « Paquet télécom » de 2009. Elle a été transposée à l'article 34 bis de la loi « informatique et liberté ». Cette obligation ne concernait jusqu'ici que les « fournisseurs de services de communications électroniques »[61]. Il faut entendre par là les FAI et les opérateurs téléphoniques. Mais la loi exclue de cette qualification les éditeurs et les hébergeurs de sites web. Lorsqu'un fournisseur de services de communication est victime d'une violation sécurité, il doit avertir « au plus vite » l'autorité nationale compétente dans le cas où des données pourraient avoir été perdues, altérées, ou divulguées.

[61] *Voir : article 32, alinéa 6 du Code des postes et des communications électroniques (CPCE)*

Si la violation de sécurité risque d'affecter les données personnelles d'un utilisateur (atteinte à la réputation, humiliation, usurpation d'identité, etc.), le fournisseur a également pour obligation de l'en informer. Ceci n'est pas nécessaire si le fournisseur a démontré à l'autorité nationale compétente que les mesures de sécurité attachées aux données les rendaient incompréhensibles pour les tiers (protocole de cryptage). Si le nombre de victimes est trop conséquent, par soucis d'économie et de simplicité, la notification peut se faire par le biais d'une communication publique.

Cette obligation traduit la volonté d'améliorer la lutte contre le piratage. En effet, la pratique la plus couramment répandue en cas de cyberattaque est de garder le silence. Les entreprises ne veulent bien évidemment pas de mauvaise publicité quant à leurs systèmes de sécurité. Ce qui a deux conséquences : la sous-estimation de l'ampleur de la cybercriminalité et l'instauration d'une « loi du silence » chez les opérateurs du numérique. Obliger ces derniers à faire preuve d'une certaine transparence, c'est se doter de meilleurs moyens de lutter contre les cybercriminels.

L'article 33 du RGPD procède à une généralisation de l'obligation de notifier les failles de sécurité à tous les responsables de traitement. On peut noter que le RGPD, contrairement à la loi « Informatique et libertés », précise le délai dans lequel la notification doit être faite. Il s'agit d'un délai de 72 heures. L'extension de cette obligation risque de nourrir beaucoup de contentieux à l'avenir. On peut se douter que les acteurs du numérique, qui auront tout à gagner à mettre en avant leur capacité à protéger les données personnelles de leurs clients, ne seront pas forcément très enclins à les informer de l'existence de failles majeures dans leurs dispositifs de sécurité. Ne pas prévoir un délai précis de notification aurait pu avoir pour conséquence de déplacer le contentieux sur ce terrain.

Par ailleurs, la notion de « violation » n'étant pas clairement définie, elle laisse la place à de très nombreux cas de figure. Par exemple, la violation peut consister tant en un piratage réseau que, de manière plus banale, en la perte de matériel informatique comportant des données personnelles (ordinateur portable, tablette, smartphone, clé USB, etc.), ou encore en une imprudence de la part du responsable de traitement pouvant permettre l'accès aux données par un tiers non autorisé. En pratique, cette obligation pourrait trouver à s'appliquer de manière récurrente chez les acteurs du numérique. De plus, la CNIL risque d'être submergée de notifications.

Cependant, l'élargissement de l'obligation de notification obligera tous les responsables de traitement à renforcer leurs mesures de sécurité. Il s'agira pour eux d'anticiper les violations et de s'organiser pour mieux pouvoir les prévenir, de mettre en place des stratégies de maîtrise des risques. Cela dans l'intérêt de la protection des données personnelles des citoyens européens.

On peut toutefois se demander si cette obligation ne cache pas, en réalité, une « obligation d'auto-dénonciation » pour les opérateurs du numérique[62]. En effet, la violation de sécurité peut autant émaner d'un tiers (identifié ou non), que du responsable de traitement lui-même, en cas d'erreur ou d'une fausse manipulation. Dans ce cas, le responsable de traitement doit se signaler à la CNIL comme étant la victime d'une violation, bien qu'il en soit lui-même l'auteur. La victime s'expose alors à ce que soient constatés des manquements à son obligation de sécurité.

Le responsable de traitement pourra donc se voir reprocher son silence s'il ne notifie pas une violation à la CNIL mais également un défaut de sécurité s'il le fait. Espérons alors que la CNIL parvienne à faire la part des choses et se serve de ces notifications pour aider les opérateurs à élever leur niveau de sécurité. On pourrait également imaginer que la CNIL adopte une approche pragmatique, se basant sur la répétition des notifications chez un même responsable de traitement pour en conclure à l'existence d'un manquement de sa part à l'obligation de sécurité. Des violations récurrentes, traduiraient ainsi la faiblesse des moyens mis en place pour assurer la sécurité des données.

§2. L'extension de la responsabilité dans le cadre du traitement des données personnelles.

Qu'il s'agisse d'aller chercher la responsabilité d'un responsable de traitement basé à l'extérieur à l'Union européenne (A), ou d'une pluralité d'intervenants participant à un même traitement (B), la responsabilité des opérateurs amenés à utiliser les données personnelles des citoyens européens a été considérablement étendue sous l'influence du droit européen.

[62] *Arnaud Tessalonikos, « La notifications des failles de sécurité : vers une obligation de dénonciation ? », Expertises des systèmes d'information, mai 2013, page 178*

A. La responsabilité de l'opérateur établi en dehors du territoire européen.

Il résulte de l'article 5 de la loi « Informatique et libertés » que ses dispositions ne sont pas opposables au responsable de traitement basé en dehors de l'Union européenne et dont les moyens de traitement sont eux aussi extérieurs à l'Union. Cette limitation de compétence émane de la directive de 1995. C'est une particularité de la protection des données personnelles. Dans d'autres domaines relatifs à Internet, cette exclusion de compétence ne s'applique pas : la compétence du juge français est retenue de manière systématique.[63] Cette limitation ne s'applique pas non plus en ce qui concerne, notamment, la protection de la vie privée. Il suffit alors de fonder une action sur d'autres textes, comme l'article 9 du Code civil, pour voir le juge français retrouver sa compétence.[64]

Pour assurer une protection des données personnelles dans de telles situations, le G-29 estime que les « moyens techniques » devant être localisés sur le territoire européen peuvent consister dans des « traitements logiciels ». Ces derniers pouvant prendre la forme de cookies ou de l'exécution d'un script, opérant directement sur l'équipement de l'internaute européen. De cette manière, les droits nationaux des Etats membres de l'Union retrouveraient leur compétence de manière quasi-systématique. Selon le G-29, il en va de même pour le moteur de recherche qui cible et analyse le comportement d'un utilisateur européen pour lui proposer des publicités « personnalisées » sur le territoire européen.[65]

Cette solution n'a été appliquée par aucune des autorités des Etats-membres, qu'elle soit judiciaire ou administrative, jusqu'en 2014. Elle a alors été reprise à plusieurs reprises par diverses autorités administratives à travers l'Union puis par la Cour de Justice de l'Union européenne. La CNIL a ainsi repris cette solution, sur la base de l'utilisation de cookies par le prestataire, pour sanctionner Google sur le fondement de la protection des données personnelles. Cette sanction a été rendue à titre d'exemple, la CNIL lui ayant infligée l'amende la plus élevée possible, soit 150.000€.[66]

---

[63] *Voir par exemple : Cass. 1ère ch. Civile, 9 décembre 2003, Castelbanch c/ Champagne Louis Roderer*

[64] *Voir par exemple : Ordonnance de référé, TGI Paris, 19 octobre 2006, Mme H.P. c/ Google France*

[65] *Avis G-29 n° 1/2008 du 4 avril 2008 sur les aspects de la protection des données liées aux moteurs de recherche*

[66] *formation restreinte CNIL, Délibération n°2013-420 du 3 janvier 2014*

Si cette somme ne vient pas perturber le géant du numérique, elle est tout de même venue participer à un mouvement de répression des entreprises extérieures à l'Union. La CNIL se place alors dans la continuité d'une décision de son homologue espagnole qui avait déjà condamné Google a une amende de 900.000€ le 18 décembre 2013. Ce mouvement, visant à mettre un terme à l'extraterritorialité des responsables de traitement, a été rejoint par les CNIL néerlandaises et belges.

De son côté, la Cour de justice a également penché en faveur de la responsabilité d'un prestataire établi en dehors de l'Union lors de son désormais très célèbre arrêt « Google Spain ».[67] Pour ce faire, la Cour a estimé que les filiales européennes de la firme, bien qu'elles n'aient qu'un rôle commercial et n'entrent pas, de ce fait, dans le processus de traitement de données personnelles, devaient être considérées comme un établissement européen de Google Inc. La Cour a alors confirmé l'application de la directive 1995 et donc du droit national - en l'espèce espagnol - aux prestataires basés en dehors de l'Union européenne mais y possédant un établissement. De plus, elle a ajouté que le fait d'afficher des publicités ciblées en fonction des recherches des utilisateurs constituait effectivement un traitement de données personnelles réalisé sur le territoire européen, les droits nationaux retrouvant alors leur compétence.

Pour sa part, le RGPD a consacré cette solution prétorienne dans son article 3. Celui-ci opère en effet un élargissement du champ territorial de ses dispositions par rapport à la directive de 1995. Dorénavant, les responsables de traitement et sous-traitants disposant d'un établissement dans l'Union se verront appliquer la protection européenne des données personnelles, même si le traitement est réalisé dans un Etat tiers. Le règlement trouve également à s'appliquer, lorsque le traitement vise des citoyens européens ou s'il est en lien avec des biens ou services dispensés, même gratuitement, sur le territoire européen. Le responsable de traitement devra, dans ce cas, désigner un représentant établi sur le territoire de l'UE.

L'extension du champ d'application des dispositions « informatique et libertés » permettra la diffusion de la protection européenne dans d'autres Etats. En effet, les opérateurs du numériques qui ont une activité en Europe vont devoir mettre à jour leurs pratiques et se conformer à la protection européenne.

[67] *Arrêt CJUE, 13 mai 2014, n° C131/12, dit « Google Spain »*

B. *Vers une responsabilité étendue à tous les participants au processus de traitement de données personnelles ?*

Pour rappel, le responsable de traitement est la personne ou l'organisme doté des pouvoirs décisionnels quant au traitement : il en est à l'origine et en définit les modalités et les finalités. C'est lui seul qui est visé par les dispositions de la directive de 1995 et ainsi, par les dispositions de la loi « Informatique et libertés ». C'est ainsi à lui seul qu'incombent les différentes obligations afférentes à la protection des données personnelles, à lui seul que revient l'accomplissement du formalisme nécessaire à la mise en place d'un traitement et c'est encore sur lui seul que pèsent les potentielles sanctions encourues en cas de manquement au dispositif légal.

D'un autre côté, toute personne traitant des données personnelles pour le compte d'un responsable de traitement est considérée comme sous-traitant. Ce dernier doit apporter des garanties quant à sa capacité à recevoir les données et à en assurer la sécurité et la confidentialité. Le responsable du traitement doit, de son côté, veiller à l'effectivité des mesures de sécurité employées par le sous-traitant. Le recours à un sous-traitant n'enlève rien aux obligations légales mises à la charge du responsable du traitement. Le contrat le liant au sous-traitant doit indiquer les obligations de ce dernier, qui n'est tenu qu'à une responsabilité contractuelle puisqu'il n'a aucune influence sur les finalités ou sur les moyens mis en œuvre pour réaliser le traitement. C'est donc le responsable du traitement qui obligé de réparer le préjudice subi par la victime d'un manquement à la place du sous-traitant à moins que ce celui-ci n'ait méconnu les dispositions légales ou le contenu du contrat de sous-traitance, conformément à l'article 35 de la loi « Informatique et libertés ».

La question de la responsabilité du donneur d'ordre a fait l'objet de vifs débats au cours de la rédaction du règlement du 27 avril 2016 du fait de la divergence des droits des différents Etats membres dans ce type de configuration. C'est finalement une solution similaire à celle proposée par la loi « Informatique et libertés » qui a été retenue à l'article 82 du RGPD. De cette manière, le recours à un sous-traitant est encadré pour que le responsable s'assure lui-même que les données personnelles soient biens utilisées pour un traitement déterminé et qu'elles ne soient pas réutilisées ou revendues par la suite. Le sous-traitant ne doit pouvoir manipuler les données que dans la limite des instructions qui lui ont été transmises par le responsable du traitement. Il

reste toujours soumis au mécanisme général de la responsabilité délictuelle (article 1382) et ne commettre impunément d'abus dans le traitement des données qui lui sont confiées.

L'article 82 du RGPD envisage également l'hypothèse dans laquelle plusieurs responsables de traitement concourent à la réalisation d'une même opération. La répartition de leur responsabilité doit être prévue par contrat (sauf dans les cas où la loi l'assure elle-même). Les personnes concernées peuvent cependant faire valoir leurs droits indifféremment auprès de chaque responsable. Chacun d'entre eux pourra donc être amené à devoir indemniser l'intégralité du préjudice subi par la victime du manquement, à charge pour lui d'exercer par la suite une action récursoire contre les autres. Il s'agit de ne pas pénaliser les personnes concernées en permettant aux responsables de se cacher les uns derrière les autres et de se renvoyer la balle indéfiniment. La personne concernée doit pouvoir faire valoir ses droits de manière effective. Ce n'est pas à elle d'écumer le contrat liant les responsables de traitement pour savoir vers qui elle doit se tourner pour exercer ses droits (effacement ou opposition, par exemple), ou pour obtenir réparation en cas de violation de ses libertés.

Chapitre 2 : La collaboration des institutions de régulation à la protection des données personnelles.

Pour être assurée de manière efficace, la régulation des traitements des données personnelles des citoyens européens ne peut se restreindre à l'énonciation de droits accordés aux individus et d'obligations imposées aux responsables de traitement. Elle nécessite également l'intervention d'institutions, nationales ou européennes, qui auront la charge de veiller à sa bonne application et d'assurer sa cohérence au niveau européen.

Leur rôle peut alors varier. Il peut s'agir de participer à la production des normes, en assistant les législateurs nationaux ou européens, ou encore de donner des avis sur des sujets touchant à la protection des données personnelles. Il peut également s'agir de prendre part à la régulation en assurant son effectivité. Ces intervenants doivent être vus comme les accompagnateurs des opérateurs numériques, qui les aide à se mettre en conformité avec les dispositions « informatiques et libertés ». Ces institutions peuvent encore avoir un rôle de contrôle et de sanction des pratiques des organismes de traitement.

En France, la CNIL a été créée très tôt par la loi « Informatique et libertés » de 1978. Son rôle est d'assurer l'application des dispositions législatives par les responsables de traitement mais également de sensibiliser le public, de l'éduquer et ainsi chercher à lui donner une meilleure maîtrise de ses données personnelles.

Les autorités nationales de régulation ont été rendues obligatoires pour tous les Etats membres de l'Union par la directive de 1995. Leur participation à la protection des données personnelles est significative (I). Mais ces autorités nationales ne sont pas les seules à intervenir dans le processus de régulation. Le droit européen a également créé d'autres institutions et a accentué, au fil du temps, leurs prérogatives (II). Il en va ainsi, notamment, pour le délégué à la protection des données personnelles qui se voit reconnaître un rôle considérable dans le processus de régulation par le règlement du 27 avril 2016.

I. L’intervention de la Commission nationale de l’informatique et des libertés.

Très tôt, la loi « informatique et libertés » a créé une autorité administrative indépendante qui a pour but d'assurer le respect des droits des personnes et des obligations mises à la charge du responsable de traitement : la Commission nationale de l'informatique et des libertés. Initialement, la CNIL était « *chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et contrôlant les applications de l'informatique aux traitements des informations nominatives* ».[68] La transposition de la Directive de 1995 opérée par la Loi de 2004 a permis d'accroître les prérogatives de la CNIL. En effet, si son rôle se cantonnait auparavant à un aspect procédural (formalités nécessaires au traitement), elle est désormais dotée de pouvoirs de contrôle et de sanction. La CNIL effectue de cette manière un contrôle aussi bien a priori qu'à posteriori des traitements de données à caractère personnel. De plus, elle peut décider de sanctionner un responsable de traitement qui ne respecte pas les normes « informatiques et libertés » au moyen d’une procédure particulière, cherchant davantage la mise en conformité d’un manquement que la sanction de l’opérateur. Le rôle de la CNIL est également d'accompagner les entreprises dans la construction de leurs politiques de protection des données. Elle peut ainsi donner son avis sur la conformité de règles professionnelles, de systèmes ou de procédures via lesquelles l'entreprise cherche à mieux respecter les dispositions « informatique et libertés ». En outre, et comme nous le verrons par la suite, la CNIL a pour objectif de diffuser une certaine éthique en matière de données personnelles et de sensibiliser le public et les opérateurs du numérique.

Actuellement, l’une des principales fonctions de la CNIL est de recevoir les formalités préalables imposées aux responsables de traitement (§1). Mais la CNIL doit également s’assurer du respect des libertés fondamentales des personnes dont les données ont été collectées, disposant de ce fait d’un pouvoir de contrôle et de sanction (§2). Enfin, suite à la recherche d’une protection harmonisée à l’échelle européenne, le règlement du 27 avril 2016 prévoit un dispositif de cohérence et de coopération des différentes autorités nationales de régulation (§3).

[68] *Article 6 du texte initial de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

§1. Les formalités préalables devant être remplies par les responsables de traitement.

En principe, tout fichier ou traitement comportant des données à caractère personnel doit, préalablement à sa mise en œuvre, être déclaré à la CNIL. Cette obligation de déclaration s'applique en principe à tous les opérateurs du secteur du numérique, qu'ils proviennent du secteur public ou privé. Des dispenses peuvent toutefois être organisées dans certains cas relevant de l'intelligence nationale. Le non-respect de ces formalités légales fait l'objet de l'article 226-16 Code pénal et expose son auteur à une sanction pouvant s'élever à 300.000€ d'amende (pouvant être portée à 1.500.000€ pour une personne morale) et à 5 ans d'emprisonnement, comme il est d'usage dans la régulation du traitement des données personnelles.

Les modalités de déclaration à la CNIL peuvent prendre plusieurs formes selon le contenu du fichier, les finalités du traitement et les risques induits pour les personnes concernées. Ainsi, la déclaration normale est le principe en termes de formalité (A). Il doit y être procédé dès lors que le fichier ou traitement ne se place pas dans le cadre d'une procédure spéciale. Dans de telles circonstances, les formalités peuvent être assouplies (B) ou alourdies (C). En cas de doute sur la qualification des données concernées ou de la finalité du traitement, et donc d'incertitude quant au régime déclaratif à accomplir, le responsable du traitement ou le propriétaire du fichier est invité à recourir à une déclaration simple auprès de la CNIL qui se chargera alors elle-même de la qualification du dossier.[69]

A. La déclaration normale : procédure « commune » de formalité préalable.

Pour commencer, la déclaration dite « normale » constitue la voie commune en matière de formalité préalable. Elle amène le responsable de traitement à donner à la CNIL de nombreuses informations relatives au traitement. La déclaration doit ainsi comporter la finalité du traitement, les personnes concernées par le traitement, les technologies utilisées (géolocalisation, vidéosurveillance, cookies, etc.), les catégories de données traitées (finances, environnement, vie personnelle ou professionnelle, etc.), les données sensibles qui pourraient

[69] *Jérôme Lefort, Marion Hainez et Marine Chatelet, « Gérer, sécuriser et valoriser ses données personnelles des collectivités territoriales », Territorial Editions, 2015, p. 27*

être traitées, les mesures de sécurité mises en œuvre pour assurer la protection des données. Elle doit également indiquer si les données seront amenées à être exportées dans des pays assurant un niveau de protection adéquat. Si le pays n'assure pas un tel niveau de protection, le transfert devra faire l'objet d'une demande d'autorisation, comme nous le verrons ci-après. De la même manière, le responsable de traitement doit signaler s'il envisage d'éventuelles interconnexions de fichiers répondant à la même finalité. Si les interconnexions concernent des fichiers voués à d'autres finalités que celle du traitement initial, une demande d'autorisation devra, là encore, être formulée. Enfin, il doit également faire connaître la manière dont il compte informer les personnes concernées de la collecte de leurs données, du traitement mis en place et des droits qu'elles détiennent.

B. *L'assouplissement des formalités en présence de risques moindre pour les personnes concernées.*

Lorsque le traitement envisagé ne présente pas de risques conséquents pour les individus dont les données personnelles seront utilisées, le responsable de traitement peut être soit dispensé de remplir une quelconque formalité (1), soit soumis à procédure simplifiée (2). Par ailleurs, par soucis de simplicité, la CNIL peut décider de mettre en place une procédure d'autorisation unique (3).

1) La dispense de déclaration préalable.

Conformément à l'article 22 de la loi « Informatique et libertés », des fichiers ou traitements de données personnelles ne portant pas atteinte à la vie privée et aux libertés fondamentales des personnes concernées sont dispensés de déclaration à la CNIL. De la même manière, des dispenses sectorielles ont été mises en place par la CNIL au cours de différentes délibérations et ce, conformément à l'article 24 de la même loi. Ces dispenses concernent pour la plupart l'administration, on y retrouve, entre autres, la gestion de la comptabilité[70], la gestion des rémunérations du personnel de la collectivité territoriale (dispense n°1), le traitement des fournisseurs de la collectivité territoriale (dispense n° 4), le traitement dématérialisé des marchés publics (dispense n°3), etc.

[70] *Délibération CNIL n° 80-34 du 21 octobre 1980*

D’autres dispenses ont été mises en place par la loi elle-même. Sont ainsi dispensés le traitement « *ayant pour seul objet la tenue d'un registre exclusivement destiné à l'information du public et est ouvert à la consultation de celui-ci* »,[71] mais également celui mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical. Cette dispense est cependant encadrée de manière stricte, en raison de la sensibilité des données susceptibles d’être collectées par ce type d’organisme. Le registre doit ainsi être destiné à l’information du public et ouvert à la consultation sous réserve qu’il ne concerne que des membres de l’association et ne comportant que des données non communiquées à des tiers. Une exception a également été aménagée dans le cadre des traitements réalisés à des fins d’archivage. Par ailleurs, sont dispensés de déclarations préalables les responsables de traitement qui ont nommé un « Correspondant Informatique et libertés ». Cependant, cette dispense ne s’étend pas aux traitements pour lesquels une demande d'autorisation ou d'avis est nécessaire.

2) La déclaration simplifiée.

Sur le fondement de l’article 24 de la loi « Informatique et libertés », la CNIL a mis en place un dispositif de simplification des formalités de déclaration. Cette simplification s’applique aux traitements qui ne sont, encore une fois, pas susceptibles de porter atteinte aux libertés des personnes concernées. Sur la base de normes simplifiées et d’un engagement de conformité, le responsable de traitement peut recourir à une simple « déclaration de conformité ». Dans ce cas, les fichiers ou traitements concernés doivent respecter à la lettre les normes établies par la CNIL. Lorsqu'une déclaration simplifiée est déposée, un récépissé est remis au responsable du traitement. Il lui permettra de mettre en œuvre le traitement dès la réception. Dans la sphère administrative, cette procédure allégée trouve à s’appliquer, par exemple, pour des traitements relatifs aux fichiers du cadastre (norme simplifiée n° 44), à la gestion de l’état civil (norme simplifiée n° 43), à l’analyse de la consommation de gaz, d’eau, d’électricité et des redevances d’assainissement (norme simplifiée n° 8), au logement social (norme simplifiée n° 20), ou encore à la gestion des écoles maternelles et élémentaires (norme simplifiée n° 33). Dans le secteur privé, la seule déclaration préalable peut être nécessaire pour des traitements visant, par exemple, à la gestion du personnel, à la tenue des comptes bancaires, ou à la gestion des fichiers clients.

[71] *Article 36 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

3) La mise en place d'une procédure de déclaration unique par la CNIL.

La CNIL peut procéder à une autorisation globale concernant des traitements du même type par une décision unique. Les traitements concernés doivent alors obéir aux mêmes finalités, opérer sur données de même catégorie et viser les mêmes destinataires, ou catégories de destinataires. Dans ce cas, le responsable qui procède à un nouveau traitement entrant dans la catégorie ciblée par l'autorisation unique n'aura plus qu'à présenter à la CNIL un engagement de conformité. Il doit ainsi s'engager à respecter les normes établies dans l'acte d'autorisation unique. Cette procédure permet de simplifier de manière significative les formalités légales nécessaires à la mise en œuvre d'un traitement de données à caractère personnel. La CNIL a donc la possibilité d'éditer une sorte de règlement d'exemption par catégorie de traitements.

C. L'alourdissement des formalités en cas de traitement à risques.

Face à des traitements présentant des risques pour les libertés fondamentales des personnes concernées, les formalités préalables sont alourdies. Le traitement envisagé peut donc faire l'objet d'une demande d'autorisation ou d'un avis de la CNIL (1). En ce qui concerne les traitements relevant de prérogatives de puissance publique, la CNIL est amenée à intervenir dans le cadre d'un acte réglementaire unique (2).

1) La demande d'autorisation ou d'avis de la CNIL.

Afin de protéger ces personnes, l'article 25 de la loi « Informatique et libertés » a introduit une formalité particulière, plus lourde que la simple déclaration à la CNIL. Ainsi, un responsable de traitement devra recueillir préalablement l'autorisation de la CNIL chaque fois qu'il fera l'usage de données sensibles (telles que définies à l'article 8 de la même loi), biométriques, ou bien relatives à des infractions ou condamnations. L'autorisation de la CNIL sera également nécessaire pour les traitements portant sur des données génétiques (sauf s'il est opéré par un médecin ou biologiste dans le but de pratiquer de la médecine préventive, un diagnostic ou un soin), ou sur des données comportant le numéro d'inscription de personnes au répertoire national d'identification des personnes physiques ("numéro de sécurité sociale" ou NIR).[72]

[72] *Jérôme Lefort, Marion Hainez et Marine Chatelet, « Gérer, sécuriser et valoriser ses données personnelles des collectivités territoriales », Territorial Editions, 2015, page 30*

De même, le responsable de traitement devra adresser une demande d'autorisation à la CNIL lorsqu'il sera procédé à une interconnexion de fichiers répondant à des finalités différentes. De cette manière, la loi évite que le croisement de données personnelles qui, de par le développement des technologies numérique, peut rapidement devenir très intrusif et présenter un danger conséquent pour les personnes concernées (systèmes de géolocalisation, de reconnaissance biométrique, ré-identification, discrimination, etc.). Par ailleurs, et comme nous le verrons plus loin dans le développement, une autorisation de la CNIL sera également nécessaire lorsque les données personnelles feront l'objet d'un transfert vers un Etat extérieur à l'Union européenne ne proposant pas de protection adéquate aux données personnelles. Dans ce cas, le responsable de traitement devra être en mesure de garantir que les données exportées feront l'objet d'une protection équivalente au niveau de protection européen.

La CNIL dispose d'un délai de deux mois pour rendre sa décision sur le dossier lui étant présenté (ce délai peut être renouvelé par une décision motivée du Président). Si elle ne se prononce pas au terme de ce délai, l'autorisation est réputée rejetée : il s'agit d'une décision implicite de rejet rendue par une autorité administrative. Le responsable du traitement ou d'un fichier devra se conformer en tout point à l'acte règlementaire accompagnant la décision d'autorisation ou l'avis de la CNIL.

2) L'intervention de la CNIL dans le cadre d'un acte réglementaire unique.

Cette procédure est prévue à l'article 26 de la loi « Informatique et libertés » et ne concerne que les traitements réalisés par l'Etat ou par les gestionnaires de services publics. Ces traitements sont mis en place par arrêté du ministre concerné et après avis motivé de la CNIL. La CNIL est ainsi consultée sur des traitements relatifs à la sécurité de l'Etat, à la défense, à la sécurité publique, ou bien en rapport avec des infractions pénales ou l'exécution de condamnations. Si ces traitements concernent des données sensibles, ils doivent être décidés en Conseil d'Etat et sont également soumis à l'autorisation de la CNIL. L'avis que rend la CNIL doit être publié mais une dispense de publication peut être décidée lorsque le traitement concerné nécessite de rester secret. Ce « garde-fou » permet à la CNIL de limiter les traitements opérés par la puissance publique de manière à ce que les données personnelles des citoyens français ne puissent faire l'objet d'un nouveau programme SAFARI. La CNIL a, ici encore, la possibilité d'autoriser des catégories de traitements similaires par le biais d'un acte règlementaire unique, dont le fonctionnement est comparable à celui de l'autorisation unique.

§2. Les missions de contrôle et de sanction dévolues à la Commission nationale informatique et libertés.

Pour s'assurer du bon respect des dispositions légales en matière « informatique et libertés », la CNIL revêt également une casquette de « gendarme des données personnelles ». Elle a ainsi la possibilité de réaliser des contrôles quant aux pratiques des responsables de traitement (A) et dispose également de la capacité de sanctionner leurs manquements (B).

A. Les pouvoirs de contrôles dévolus à la CNIL.

L'article 11 de la « Informatique et libertés » investit la CNIL du pouvoir de « *procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous les documents ou supports d'information utiles à ses missions* ». Les responsables de traitement visés par ces mesures de contrôle ont l'obligation de collaborer avec la CNIL. Cette obligation résulte de l'article 21 de la même loi. De la même manière, ils doivent s'abstenir d'entraver l'action de la CNIL. Les entraves peuvent être constituées par le fait de s'opposer au contrôle, de dissimuler, détruire ou refuser de communiquer des documents utiles, ou encore de fournir des informations erronées ou non pertinentes. Dans le cas contraire, ils pourraient se voir sanctionnés d'un an d'emprisonnement et de 15.000€ d'amende, conformément à l'article 51 de la loi.

Pour effectuer ces contrôles, les agents de la CNIL peuvent se déplacer dans les locaux du responsable de traitement (hormis les domiciles privés). Ils peuvent également procéder à des contrôles en ligne et constater des manquements sur le web sans avoir à en informer au préalable le responsable de traitement (usage de cookies, de traceurs, confidentialité des données collectées, sécurité des formulaires, présence des mentions obligatoires ou de failles de sécurité, etc.). La limite de ce contrôle en ligne se matérialise dans le fait que les agents de la CNIL ne peuvent pas pirater les systèmes de sécurité pour accéder aux données non rendues publiques. Le responsable d'un traitement suspecté de ne pas respecter les dispositions légales n'a pas à être prévenu de l'occurrence d'un contrôle. Mais il peut tout de même s'opposer à ce qu'il soit procédé au contrôle lorsque celui-ci est initié. La CNIL devra alors saisir le juge des libertés pour pouvoir réaliser le contrôle.

Au titre de son pouvoir de contrôle, la CNIL a annoncé, le 12 mai 2016, son programme de contrôle pour l'année à venir. La CNIL a ainsi indiqué qu'elle procèderait à plus de 400 contrôles sur place, en ligne, sur pièce ou sur audition. Dans son viseur, les entreprises de courtage de données ou « Data Brokers ». Ce sont des opérateurs agissant comme intermédiaires entre les entreprises qui recueillent des données et celles qui souhaitent les acquérir pour les utiliser dans le cadre de leur activité. Les courtiers prélèvent les données (en général sur le réseau) et les rassemblent par catégories en vue de constituer un fichier structuré. Toutes les catégories de données sont ciblées (sensibles ou non, financières, comportementales, bien-être, etc.). La CNIL a annoncé qu'elle serait particulièrement vigilante sur la pertinence des données, les mesures de sécurité mises en place ainsi que sur le respect de l'information et du consentement des personnes concernées. Cette suspicion de la CNIL s'explique par le fait qu'il n'existe aucun point de contact entre les individus et les « Data Brokers », ce qui rend l'expression du consentement relativement complexe.

Par ailleurs, les acheteurs doivent eux aussi prendre garde. En effet, l'usage qu'ils feront des données personnelles les conduira à devenir eux-mêmes des responsables de traitement et à se voir reprocher, à ce titre, des manquements issus de la collecte initiale (collecte illicite, détournement de finalité, etc.). Les acheteurs ne peuvent pas échapper à cette responsabilité, même par la voie contractuelle. L'annonce de sa politique de contrôle par la CNIL risque donc d'avoir un effet néfaste sur l'activité de courtage de données.[73]

Une telle situation risque également d'affirmer le monopole des grandes entreprises du numérique en matière de commercialisation de données. En effet, ces entreprises collectent elles-mêmes les données personnelles avant de les revendre, ce qui leur permet de maîtriser la conformité des procédés de collecte. Or, cette maîtrise échappe souvent aux simples courtiers. Les acheteurs pourraient donc être amenés à leur préférer des vendeurs eux-mêmes responsables de traitement qui peuvent assurer la conformité des modalités de la collecte. Ils s'assureraient ainsi davantage de ne pas être sanctionnés par la suite pour le non-respect des dispositions « informatique et libertés ».

[73] *Amira BOUNEDJOUM, « La commercialisation des données personnelles dans la ligne de mire de la CNIL ! ». Voir : http://www.lesechos.fr/idees-debats/cercle/cercle-157928-la-commercialisation-des-donnees-personnelles-dans-la-ligne-de-mire-de-la-cnil-2010000.php*

Pour finir, le contrôle de la CNIL peut se solder par des recommandations ou, si des manquements graves ont été découverts, par une mise en demeure de cesser le traitement ou de se mettre en conformité. Si le responsable de traitement ne s'exécute pas, une procédure de sanction pourra être lancée à son encontre.

B. Les pouvoirs de sanctions dévolus à la CNIL.

Si l'application des peines planchers prévues par le Code pénal n'est pas assurée par la juridiction pénale, celle-ci n'est pas la seule dotée d'un pouvoir de sanction à cet égard. Initialement, la CNIL ne pouvait qu'adjoindre le responsable d'un traitement violant les obligations légales à des « *mesures de sécurité pouvant aller jusqu'à la destruction des supports d'information* », ou en avertir le Parquet en vue de poursuites pénales.[74]. Depuis la transposition de la Directive de 1995 opérée par la Loi du 6 août 2004, la CNIL s'est vue dotée d'un véritable pouvoir de sanction. Le pouvoir de sanction accordé à la CNIL sur la base de la Directive de 1995 a été débattu et a déjà eu l'occasion d'opposer la doctrine. Cependant, force est de constater qu'en matière de protection des données personnelles, la CNIL est à la fois plus sensibilisée à la protection du droit des personnes que ne le sont les juges. De plus, elle dispose également d'une plus grande capacité d'expertise technique.

La procédure de sanction doit nécessairement passer par l'avertissement ou la mise en demeure du responsable de traitement de se mettre en conformité avec les dispositions légales. C'est seulement si ce dernier ne s'exécute pas que la CNIL pourra prononcer une sanction pécuniaire ou l'obliger à faire cesser le traitement, conformément aux dispositions de l'article 45 de la loi « Informatique et libertés ». Jusqu'ici, le montant de l'amende administrative ne pouvait pas excéder 150.000€, sauf en cas de récidive où il pouvait être porté à un maximum de 300.000€. Les sanctions prononcées par la CNIL peuvent être nettement supérieures à celles prononcés par les tribunaux pour des faits comparables. Cependant, le montant maximal de 150.000€ n'a été prononcé qu'une seule fois, contre Google.[75]

Les amendes administratives peuvent parfois être plus sévères que ne le sont les dispositions du Code pénal. Ainsi, la CNIL a pu sanctionner le Crédit Lyonnais pour ne pas avoir mis à jour

---

[74] Article 21, alinéas 3 et 4 du texte initial de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[75] Fabrice Mattatia, « Le droit des données personnelles », Eyrolles 2ème édition, 2015, p. 197

des fichiers clients tout en prétextant le respect du secret bancaire pour ne pas coopérer avec elle. L'infraction qui est considérée par l'article R. 625-12 du Code pénal comme une contravention de 5ème classe (punie d'une amende de 1.500€ maximum) s'est retrouvée sanctionnée par la CNIL d'une amende administrative d'un montant de 45.000€.[76] Pourtant la CNIL a rarement recours à ces sanctions puisque la logique de la loi « Informatique et libertés » repose plus sur une approche préventive. L'attitude du responsable de traitement et sa volonté de coopérer sont donc des paramètres déterminants de la sanction. Celle-ci sera donc alourdie en cas de « mauvaise foi » de sa part. La CNIL doit alors être perçue comme un « instituteur informatique et libertés ». Elle fait ainsi davantage preuve de pédagogie que d'autoritarisme, préférant pointer du doigt les mauvaises pratiques pour permettre aux opérateurs du numérique d'y remédier qu'adopter une approche disciplinaire la conduisant à sanctionner les « mauvais élèves » de manière systématique. La procédure entourant la sanction démontre bien cette logique de dialogue et d'éducation, se soldant souvent par un règlement des litiges à l'amiable.

Toutefois, les sanctions pouvant être prononcées par la CNIL restent dérisoires pour les entreprises et peuvent être inférieures aux coûts d'une remise à niveau du procédé de traitement. Il pouvait alors sembler opportun d'augmenter les pouvoirs de sanction des autorités nationales européennes. Il paraît également nécessaire d'harmoniser ces pouvoirs de sanction afin de ne pas créer de déséquilibre entre les acteurs du numérique sur le territoire européen. De ce fait, l'article 83 du RGPD réaffirme le pouvoir de sanction des autorités nationales de régulation. Le calcul du montant de ces amendes doit prendre en compte les circonstances et l'importance du manquement observé. Elles doivent être « effectives », « proportionnées » et « dissuasives ». Après négociations, le montant des amendes administratives a été fortement rehaussé par rapport à ce que prévoyait la directive de 1995. En effet, les amendes peuvent désormais aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial réalisé par une entreprise (si ce montant est supérieur à 20 millions d'euros). Ainsi, les autorités nationales ont désormais la possibilité de faire de ces sanctions de véritables exemples pour tous les acteurs du secteur du numérique. Elles peuvent également pénaliser réellement les plus gros d'entre eux, grâce à l'indexation du montant de l'amende sur le chiffre d'affaires. Dorénavant, les coûts de mise en conformité ne pourront donc plus être supérieurs aux amendes infligées.

[76] *Délibération CNIL n° 2006-174 du 28 juin 2006*

§3. L'insertion d'un mécanisme de cohérence entre les autorités nationales européennes.

Une des heureuses conséquences de la construction du marché unique demeure la multiplication des entreprises établies dans plusieurs Etats membres de l'Union européenne. Mais, bien que la question du droit applicable soit résolue par l'adoption d'un Règlement européen, cela pose des problèmes de compétence pour les autorités nationales de contrôle. Ainsi, dans le cadre de la coopération des autorités nationales, le RGPD introduit la notion d' « établissement principal » du responsable de traitement ou du sous-traitant. Le lieu de l'établissement principal devra alors être apprécié selon la localisation du centre névralgique du traitement. Il s'agit de l'endroit où les décisions effectives sont prises. Les autorités nationales ont critiqué cette notion en craignant que les entreprises ne puissent pratiquer une sorte de « forum shopping » en choisissant d'établir leur établissement principal dans des Etats membres où les autorités de contrôle seraient plus conciliantes. Cependant, l'appréciation de l'établissement principal est faite à partir d'une situation de fait et non de droit. Ce qui, certes, est source d'insécurité juridique, mais réduit la marge de manœuvre des responsables de traitement.

Par ailleurs, le RGPD a construit un « mécanisme de cohérence » régissant les rapports des autorités nationales dans le cadre de dossiers transnationaux. On retrouve ce mécanisme à l'article 60 du RGPD. Celui-ci créé alors le concept d'autorité « chef de file ». Il s'agit de l'autorité de l'Etat dans lequel le responsable de traitement a établi son établissement principal. En principe, le « chef de file » en est le seul interlocuteur, conformément à l'article 56 du RGPD. Sa décision est alors applicable dans l'ensemble du territoire européen. Mais, par exception, les autorités nationales retrouveront leur compétence lorsqu'une violation du Règlement ne concernera que leur propre Etat. Les autorités nationales doivent assurer entre elles une coopération « loyale ». Ainsi, les autorités doivent s'échanger des informations et peuvent mener des opérations conjointes. D'autre part, cela implique la recherche d'un consensus entre l'autorité « chef de file » et les autres autorités nationales impliquées dans un même dossier. De ce fait, l'autorité « chef de file » doit informer les autres autorités nationales de son projet de décision et recueillir leurs avis et objections éventuelles. Toutefois, en cas d'urgence, une autorité nationale peut prendre, seule, des mesures provisoires sans appliquer le mécanisme de cohérence qui l'obligerait à attendre l'avis du « chef de file » ou des autres autorités nationales.

II. Les autres autorités intervenant dans le processus de régulation.

Outre les autorités nationales de régulation, d'autres acteurs sont amenés à participer au processus de régulation des traitements de données personnelles. Ainsi, le RGPD renforce le rôle du délégué à la protection des données qui en est désormais au cœur (§1) ainsi que celui du G-29, qui s'appellera désormais « Comité européen de la protection des données » (§2). Enfin, le contrôleur européen de la protection des données est amené à assurer la régulation de l'utilisation de données personnelles par les institutions de l'Union européenne (§3).

§1. Le délégué à la protection des données : nouvel acteur-clé de la régulation.

La directive de 1995 a institutionnalisé un délégué à la protection des données personnelles assurant un lien entre les responsables de traitement et les autorités nationales de régulation. Ce qui a donné naissance au « Correspondant informatique et libertés » en France (A). Le règlement du 27 avril 2016 a généralisé sa désignation, élargi ses compétences pour finalement le placer au cœur de la régulation des traitements de données à caractère personnel (B).

A. Le Correspondant informatique et libertés : un relai dans la protection des données personnelles.

Le « Correspondant informatique et libertés » (CIL) a été institué en 2004, à l'occasion de la refonte de la loi « Informatique et libertés ». Il fait désormais l'objet de l'article 22 de la loi. Il s'agit d'un interlocuteur privilégié, faisant office de relai entre le responsable de traitement et la CNIL. Sa raison d'être est de prévenir les risques dans l'application de la loi. Aucun diplôme spécifique n'est exigé par la loi pour pouvoir exercer la fonction de CIL. Cette dernière exige simplement que la personne « *bénéficie des qualifications requises pour exercer ses missions* ». Par ailleurs, le CIL exerçant ses fonctions en toute indépendance, il dispose d'un droit d'alerte lui donnant la possibilité d'avertir la CNIL de difficultés qu'il pourrait rencontrer à l'occasion de l'exercice de ses missions. Il pourra faire usage de son droit d'alerte s'il ne parvient pas à trouver de solution avec le responsable de traitement.

La désignation du CIL est facultative mais elle permet à l'organisme de traitement de se dédouaner de la déclaration (simplifiée ou non) d'une large part des fichiers comportant des données personnelles, en dehors de ceux nécessitant une demande d'autorisation ou d'avis de la CNIL. La désignation d'un CIL est source de sécurité juridique et informatique. En effet, il a pour missions de vérifier la licéité du traitement et de l'effectivité des mesures de sécurité. Cela permet au responsable de traitement de réduire considérablement les risques de contentieux en matière de données personnelles. Avoir recours aux services d'un CIL permet également la diffusion de la « culture informatique et libertés ». La CNIL estime en effet que « *désigner un correspondant permet certes de bénéficier d'un allègement des formalités déclaratives mais surtout de s'assurer que l'informatique de l'organisation se développera sans danger pour les droits des usagers, des clients et des salariés* ».[77]

Plus précisément, les missions dévolues au CIL sont d'accompagner l'organisme dans tout ce qui à trait aux données personnelles. Il doit tout d'abord assurer la tenue d'un registre de suivi des traitements automatisés, ce qui permet d'assurer une certaine transparence et une traçabilité des données. Il prend en charge le traitement des requêtes et des réclamations, aux fins de transmission aux services concernés tout en leur apportant son expertise. Il veille au respect des droits d'accès, d'opposition et d'information au sein de l'organisme pour lequel il travaille. Le CIL est également chargé de préparer et suivre les formalités légales dont l'organisme n'est pas exonéré. Enfin, ses principales tâches sont le conseil, l'information et la veille. Il doit alors régir la mise en place d'une politique interne en matière de protection des données personnelles. Cela passe par la sensibilisation aux enjeux de la mise en conformité (à travers des supports d'informations, codes de conduite, des guides internes, etc.). Toutefois, il est apparu que, dans la majorité des cas, seules les grandes entreprises et les collectivités locales avaient recours à la nomination d'un CIL puisque sensibilisées aux dispositions légales en matière d'informatique et de libertés. Le gain obtenu (dispense de déclaration) étant compensé par l'obligation de déclarer les traitements au CIL lui-même au lieu de la CNIL. Il a ainsi pu être observé que le recours à ce médiateur a été largement ignoré par les PME ou TPE.

[77] *26éme rapport d'activité de la CNIL, 2005. Voir : http://www.ladocumentationfrancaise.fr/rapports-publics/064000317/*

B. Vers un « CIL 2.0 » placé au cœur de la protection des données personnelles.

L'actuel CIL fait l'objet de la section IV du RGPD (articles 37, 38 et 39). Il deviendra le « Délégué à la protection des données » ou « Data Protection Officer » (DPO) et ses responsabilités seront accrues. Compte tenu de ses missions et de son rôle de « lien » entre les acteurs du numérique et les autorités de contrôle, le DPO est placé au centre du mécanisme de l'autorégulation voulu par le RGPD. Par ailleurs, l'indépendance accordée au CPO lui permettra d'être totalement autonome vis-à-vis de son/ses employeur(s). Il sera donc en capacité d'exercer ses fonctions de manière neutre et objective, sans subir aucune pression de la part du responsable de traitement.

Outre l'accompagnement des nouveaux projets et notamment la mise en place d'une protection des données dès la conception d'un produit ou service[78], il jouera une place toute particulière dans le mécanisme de conformité. Ainsi, il accompagnera le responsable de traitement pour que celui-ci puisse apporter la preuve de la conformité de ses agissements, comme nous le verrons plus tard dans ce développement. Le DPO devra alors veiller à ce que soient réalisées des analyses d'impact sur la vie privée, lorsque la situation l'exigera[79]. De plus, le DPO devra assurer la gestion des violations des droits des personnes concernées par un traitement. Au travers de ses diverses missions, il apparaît comme l'acteur clé de la conformité des pratiques des responsables de traitement au dispositif légal. C'est lui qui va coordonner et fédérer les différents moyens et instruments mis en place dans le cadre des traitements. Le DPO va donc s'inscrire en tant que « pilote de la gouvernance numérique » chez les opérateurs du numérique. De ce fait, les ressources lui étant consacrées vont devoir, elles-aussi, être revues à la hausse. On peut anticiper une forte augmentation du nombre de CPO exerçant leurs missions à temps plein. Ces derniers disposeront également d'un droit d'accès aux données, ce qui n'était pas le cas des CIL, et leur vaudra d'être soumis au secret professionnel.

L'obligation généralisée à l'ensemble des acteurs du numérique d'avoir à désigner un CPO a fait l'objet d'importantes négociations. Suite à un consensus, sa désignation est désormais rendue obligatoire pour les acteurs du service public, pour les opérateurs réalisant, à grande échelle, du profilage ou traitant, toujours en masse, des données sensibles ou rattachées à des

[78] *Voir « Privacy by design »*

[79] *Voir études d'impact ou « Privacy impact assessment »*

condamnations pénales. D'une manière concrète, ce compromis permet de toucher la quasi-totalité des entreprises numériques qui sont amenées, comme nous avons pu le voir, à brasser des quantités de données de plus en plus impressionnantes et, par voie de conséquence, de plus en plus sensibles. Rendre ce correspondant obligatoire pour le plus grand nombre paraît être une très bonne solution puisque cela permet non seulement d'assurer un haut niveau de protection des données, mais également de parvenir à une meilleure prévention des infractions. L'action du CIL évitera alors à de nombreux responsables de traitement d'être pénalisés pour leur méconnaissance du cadre légal. Qui plus est, la généralisation de la désignation du DPO permettra le sensibilisation des entreprises et donc une meilleure diffusion des bonnes pratiques. Un petit bémol réside toutefois dans le fait que le RGPD n'ait pas prévu la possibilité que les actuels CIL puissent reprendre leurs fonctions en tant que DPO. L'AFCDP[80] a donc demandé à ce que soit insérée une clause dite « du grand-père » qui permettrait aux CIL qui le souhaitent et qui détiennent les compétences nécessaires de devenir DPO. De cette manière les organismes ayant recours à leurs services pourrait capitaliser l'expérience qu'ils ont pu acquérir jusque-là.

Face aux problématiques économiques touchant les plus petites structures, le RGPD prévoit la possibilité d'avoir recours à un « DPO mutualisé » qui travaillerait en même temps pour plusieurs entreprises. La seule condition à cela est que le délégué soit facilement joignable par tous les organismes auprès desquels il intervient. De cette manière, les ressources mises en place seraient restreintes et très vite compensées par les gains engendrés par une meilleure protection des données personnelles. Le dispositif n'accentuerait alors pas de manière significative le déséquilibre entre les grands acteurs et ceux de taille plus restreinte.

§2. L'actualisation du G-29 : le nouveau Comité européen de la protection des données.

Le Comité européen de la protection des données (CEPD) est un organe de droit européen qui rassemble les directeurs des autorités de contrôle nationales. Il succède au groupe de travail « article 29 » (G-29) institué par l'article 29 de la directive de 1995.

[80] *Association qui regroupe les professionnels de la conformité Informatique et Libertés et de la protection des données personnelles*

Le G-29 n'avait qu'un rôle purement consultatif. À ce titre, il contribuait à l'élaboration de normes européennes en adoptant des recommandations. Il devait également assister la Commission et rendre des avis sur les niveaux de protection des Etats extérieurs à L'union européenne. Sa mission consistait également à conseiller la Commission européenne sur tout projet qui aurait une incidence sur la protection des données personnelles des citoyens européens. Le G-29 avait été créé pour promouvoir la coopération des autorités nationales européennes, dans le cadre de la recherche d'une application uniforme des dispositions de la directive 1995.

Le nouveau Comité européen sera, quant à lui, doté de réels pouvoirs. Son rôle ne se limitera donc pas au simple rôle de conseil de la Commission européenne alloué au G-29. Le CEPD devra approuver des clauses contractuelles types, des critères de certification, ou bien publier une liste de traitements nécessitant de réaliser une analyse d'impact. Il agira également en tant que « chef d'orchestre » des autorités nationales. Et devra, à ce titre, être consulté avant que des décisions pouvant avoir des impacts dans d'autres Etats membres ne soient prises par les autorités nationales. Ainsi, dans le cadre d'un dossier transnational, l'autorité « chef de file » devra nécessairement consulter le CEPD. Dans le cadre de l'application du mécanisme de cohérence, il pourra trancher en cas de désaccord entre plusieurs autorités nationales.

§3. Le contrôleur européen de la protection des données.

Le contrôleur européen de la protection des données ou « European data protection supervisor » (EDPS) est une autorité de contrôle indépendante instituée par le règlement du 18 décembre 2000.[81] Sa compétence est restreinte aux opérations de traitement de données personnelles opérées par les organes et institutions de l'Union européenne. Il veille à ce que ces derniers soient respectueux des dispositions du règlement. Il n'est pas compétent en ce qui concerne les traitements effectués dans les Etats membres et n'est donc pas chargé de faire appliquer la directive de 1995, bien que ses principes aient été calqués dans le règlement du 18 décembre 2000. Il est donc en quelque sorte la CNIL des institutions de l'Union. L'EDPS n'a pas été affecté par les dispositions du règlement du 27 avril 2016.

[81] *Règlement (UE) n° 45/2001/CE du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données*

L'EDPS est investi de différentes missions. Tout d'abord, il supervise le traitement des données à caractère personnel par les organes européens. Il peut, pour ce faire, s'appuyer sur le concours des délégués à la protection des données de chaque institution ou organe européen qui lui adressent des notifications et l'informent des modalités des traitements mis en œuvre. Il peut également s'appuyer sur les pouvoirs de contrôle qui lui ont été confiés. Il dispose de l'autorité nécessaire pour décider de procéder à des enquêtes et inspections au sein des organes européens. Il a également un rôle consultatif. Il conseille à ce titre l'ensemble des institutions et des organes européens quand la question des données est en jeu. Il est alors amené à intervenir dans le processus normatif auprès de la Commission européenne ou dans le processus judiciaire auprès de la CJUE. Son rôle est ainsi, au même titre que l'actuel G-29, majoritairement consultatif.

Il participe également aux balbutiements d'une prise de conscience à l'échelle internationale quant à la nécessité de la protection des données personnelles en sensibilisant certaines organisations internationales à ces problématiques. Que les institutions internationales elles-mêmes assurent une meilleure protection des données personnelles à l'occasion des traitements qu'elles sont amenées à en faire semble être un premier pas nécessaire à la mise en place d'une régulation internationale.

Par ailleurs, l'EDPS est également chargé de l'encadrement du système Eurodac.[82] Il supervise et encadre le traitement des données qui y sont centralisées. Il procède ainsi, chaque année, à des contrôles et se réunit avec les autorités nationales chargées de la protection des données personnelles pour trouver des solutions aux problèmes posés par ces traitements. Il faut préciser qu'Eurodac a été mis en place par la directive de 1995, ce qui explique la compétence des autorités nationales pour veiller à ce leurs droits nationaux soient respectés dans l'application de ce système.

Enfin, l'EDPS a un rôle de coopération et permet une plus grande cohérence de l'articulation de la protection des données personnelles à l'échelle européenne. Il coopère ainsi avec les autorités nationales de protection, de manière directe ou à travers le G-29. Il coopère également avec les organes de contrôle de la protection des données dans le cadre de la coopération policière et judiciaire dans l'union, comme Europol par exemple.

[82] *Eurodac est une base de données de l'UE qui permet de comparer les empreintes digitales d'immigrés et de demandeurs d'asile se trouvant en situation irrégulière sur le territoire des Etats membres*

Partie 2 – L'intégration des données personnelles dans le marché économique numérique.

Internet a pour pierre angulaire la confiance des internautes. Si celle-ci venait à se briser, il faudrait faire face à une crise considérable dont les conséquences économiques, sociales et politiques pourraient être catastrophiques. Aujourd'hui on peut assister à une remise en question de la liberté d'expression sur Internet. Les échanges d'opinions peuvent en souffrir, surtout lorsque les points de vues exprimés sont marginaux dans des sphères sociales ou professionnelles. On assiste à la prise de conscience qu'Internet n'est pas vraiment anonyme, d'un risque d'être entendu par des personnes ou institutions indésirables.

La captation de données par les gouvernements peut prendre de nombreux aspects. Il peut s'agir de programmes comme ECHELON (issu d'un accord entre les Etats-Unis, la Canada, le Royaume-Uni, la Nouvelle-Zélande et l'Australie) assurant la captation des données et des communications au sein de diverses infrastructures : fibre optique, câbles sous-marins (comme ceux de Google, 3ème câblo-opérateur au monde, qui assure pourtant avoir la maîtrise absolue de l'ensemble de ses systèmes de stockage). Il peut également être question de l'exploitation de failles de sécurité dans les protocoles, comme la faille « Heartland » observée dans le protocole Open SSL.[83] Il peut encore s'agir d'un programme de surveillance massive, comme le programme PRISM de la NSA. Celui-ci a permis aux autorités américaines de déchiffrer - donc d'avoir accès et de répertorier - toutes les données détenues par les GAFA sous couvert de la lutte antiterroriste (Foreign Intelligence Surveillance Act et Patriot Act). Les données détenues par les géants du numérique sont alors accessibles sans contrôle judiciaire ni protection des libertés. Par ailleurs, les données filtrées n'ont pas besoin d'être stockées sur le sol américain, il suffit qu'une société y ait des intérêts ou que l'information recherchée concerne

[83] *La faille Heartland est une faille de sécurité révélée en 2014 et présente depuis 2012. Elle a été observée dans un protocole assurant la sécurité de systèmes d'exploitation comme Android (Google) ; Linux ; OS X (Apple). Le système de chiffrement utilisé et potentiellement accessible était utilisé par la plupart des sites web sécurisés (https). Des millions de Go de données personnelles ont été détournés par l'exploitation de cette faille de sécurité*

la « conduite des affaires étrangères aux Etats-Unis ». Ce flou juridique intentionnel donne une énorme capacité de tractation aux autorités de renseignement américaines qui dépasse clairement le cadre de la lutte anticriminelle ou antiterroriste.[84]

L'éclatement au grand jour d'affaires de surveillance massive affecte de plus en plus l'opinion publique. Des problèmes de confidentialité apparaissent quant aux données recueillies par les entreprises, ce qui pourrait entamer de manière considérable le fragile lien de confiance unissant les utilisateurs aux opérateurs du numérique. Ainsi, les révélations d'Edward Snowden marquent une rupture entre les gouvernements et le secteur privé. Marc Zuckerberg, fondateur de Facebook, a récemment déclaré que « *le Gouvernement américain est devenu une menace pour l'Internet* ».[85] Face à de telles pratiques, même les organismes de régulation technique de l'Internet ont pris part au débat politique et ce, pour la première fois depuis leur création. Ils ont insisté sur le fait que les Etats ne devaient pas prendre le risque de déconstruire le web, cela pouvant se répercuter sur le fonctionnement même de nos sociétés. La question de la surveillance de masse est une réalité pour l'ensemble des opinions publiques mondiales. L'appropriation collective des technologies est remise en cause. Le grand public prend conscience que les acteurs économiques n'étaient pas forcément concernés par la protection des données de leurs usagers et que la surveillance concerne tous les citoyens et non simplement des individus « à risque », faisant l'objet d'une enquête ou de doutes sérieux. D'autre part, les contenus « sensibles » ne sont pas les seuls à pouvoir être soumis à un dispositif de surveillance : les métadonnées issues de la navigation des internautes en sont également l'objet. Les citoyens s'aperçoivent alors que les entreprises n'ont pas forcément les moyens ou la volonté de protéger leurs données face aux intrusions des gouvernements ou des pirates.

Dans le cadre de la Révolution numérique, les institutions européennes doivent alors chercher à lutter contre cette crise de confiance tout en permettant l'intégration des données personnelles dans les marchés numériques que ce soit, à l'échelle européenne, dans le « Marché unique numérique » (Chapitre 1), ou bien à une échelle plus globale, dans le marché numérique mondial (Chapitre 2).

---

[84] *Sylvie Rozenfield, « Affaire Prism : pas de souveraineté numérique sans industrie européenne du cloud computing », Expertises, juillet 2013, page 243*

[85] *Editorial de Marc Zuckerberg posté sur Facebook le 13 mars 2014*

Chapitre 1 : L'accroissement des débouchés commerciaux pour les données personnelles : l'intégration dans le « marché unique numérique ».

Les institutions européennes ont pour objectif de créer un « Marché unique numérique » visant à rassembler en seul marché numérique ceux des 28 Etats membres. Cela permettrait, selon la Commission européenne, d'engendrer 415 milliards d'euros par an et de créer des centaines de milliers d'emplois sur le territoire de l'Union. Elle estime également que 50 % des gains de productivité réalisés dans l'Union résultent des investissements dans les NTIC. La stratégie de l'Union européenne comprend un ensemble d'initiatives allant du droit d'auteur à la cyber-sécurité en passant par la protection des données personnelles. Il ne s'agit pas simplement d'améliorer la capacité d'accès du consommateur et des entreprises européennes à des produits et services numériques, mais également de « *créer un environnement propice au développement des réseaux et services numériques innovants et des conditions de concurrence équitables* ».[86]

Or, un tel développement du numérique ne peut passer que par la confiance du grand public accompagnée d'un certain niveau de sécurité offert par les entreprises du secteur. En plus de leur rôle de régulation, les institutions européennes et nationales ont conscience de la nécessité d'encourager le secteur privé à s'autoréguler et de faire de la protection des données personnelles un enjeu de compétitivité pour les opérateurs du numériques. Ces derniers seraient amenés se lancer dans une course à la transparence en la matière qui ne pourrait qu'être que bénéfique pour les citoyens européens. Cela permettrait également de promouvoir les bonnes pratiques en matière de protection des données personnelles, de leur transfert, de « Cloud computing » et de « Big Data ».

La construction d'un « Marché unique numérique » est donc l'une des priorités phares de l'Union européenne. À ce titre, la Commission européenne a lancé trois projets législatifs le 9 décembre 2015 : une Proposition de directive concernant « certains aspects des contrats de fourniture de contenu numérique » ; une autre Proposition de directive concernant « certains

[86] *« Stratégie numérique pour l'Europe », revues de la Commission européenne, série « Comprendre les politiques de l'UE », novembre 2014, p. 5 et 6*

aspects des contrats de ventes en ligne et de toute autre vente à distance de biens » ; et enfin une Proposition de règlement visant à « assurer la portabilité transfrontière des services de contenu en ligne dans le marché intérieur ». Ces Propositions visent à compenser l'échec subi par le Projet de règlement sur le droit commun européen de la vente, qui a été abandonné par la Commission faute de consensus entre les Etats membres. Il s'agit de développer le « Marché unique numérique » en minimisant les disparités observables dans le droit des contrats des Etats membres qui affectent le secteur du numérique. Cela permettrait de gagner une meilleure visibilité des régimes juridiques dans l'ensemble de l'Union européenne, aidant tant les entreprises que les consommateurs à nouer des relations commerciales transfrontalières. À travers ces propositions législatives, on peut clairement voir se dessiner un « droit du commerce et des pratiques numériques en ligne ». Naturellement les données personnelles, qu'elles soient objets ou causes de tels contrat, sont impactées par ces évolutions législatives.

Fait notable, la Proposition de directive « contenu numérique » élargit la notion de rémunération. Notion devant être entendue, au sens de l'article 57 TFUE, comme « *la contrepartie économique de la prestation en cause* ». Celle-ci étant assimilée, de manière classique, au paiement d'une somme d'argent. Dorénavant, la rémunération peut se faire par le biais des données personnelles. Il s'agit là d'une innovation législative et de la prise en compte d'une réalité trop longtemps ignorée : celle de la « fausse gratuité », illusion diffusée par nombre d'opérateurs du numérique. En effet, comme a pu le relever la Commission européenne : « *dans l'économie numérique, les acteurs du marché ont souvent et de plus en plus tendance à considérer les informations concernant les particuliers comme ayant une valeur comparable à celle de l'argent* ».[87]

D'autre part, outre la problématique de la surveillance massive percée à jour par les révélations d'Edward Snowden, un enjeu de taille est également apparu pour le secteur privé. Ainsi, le système de captation mis en place au travers des programmes PRISM ou ECHELON démontre la possibilité d'une intrusion des gouvernements et des agences de renseignement dans les systèmes de sécurité des opérateurs du secteur numérique. La sécurité des données personnelles est donc compromise à l'intérieur même des organismes assurant leur traitement. Ces derniers doivent donc faire face aux exigences de protection croissantes du grand public.

[87] *Proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique, considérant n° 13*

Ils peuvent également y voir une formidable opportunité compétitive. Toutefois, faute de moyens et de compréhension du cadre légal entourant les données personnelles, peu de petites structures construisent une véritable politique de gouvernance en la matière.

La Commission européenne et le G-29 ont alors lancé un mouvement tendant à faire de la protection des données personnelles un vecteur de différenciation et de compétitivité chez les entreprises du numérique. Par conséquent, le règlement du 27 avril 2016 recherche une meilleure intégration des données personnelles - en tant que marchandises - dans le « Marché unique numérique ». Mais cette logique économique ne doit prévaloir sur la protection des libertés fondamentales des citoyens. Le législateur européen cherche alors à développer un nouveau mécanisme, conciliant ces deux impératifs majeurs. L'objectif est de faire de la protection des données personnelles un avantage compétitif pour les responsables de traitement en les invitant à adhérer à une logique de corégulation (II). Par ailleurs, les institutions européennes cherchent également à agir sur le grand public, à le sensibiliser aux problématiques induites par l'exploitation des données personnelles et à lui redonner confiance et maîtrise dans l'univers du numérique (I).

I. Promouvoir la circulation des données personnelles en restaurant la confiance des citoyens européens.

L'intégration des données personnelles dans le « Marché unique numérique » est fondamentale car celles-ci représentent une valeur économique phénoménale et sont source d'une activité semblant aujourd'hui intarissable. De plus, les nouvelles technologies du numérique passent inéluctablement par le traitement de données personnelles. Ces dernières représentent ainsi des perspectives et des espoirs considérables, que ce soit dans une logique économique ou dans l'amélioration de la qualité de vie des citoyens européens.

Pourtant, une étude de la Commission européenne[88] laisse apparaître que pour 57 % des Européens, la divulgation d'informations à caractère personnel pose un réel problème. Par ailleurs, 70 % d'entre eux sont préoccupés à l'idée que des entreprises puissent utiliser des informations à des fins autres que celles pour lesquelles elles ont été collectées. Ainsi, seulement 15 % des européens ont le sentiment de contrôler totalement les informations qu'ils fournissent en ligne. D'un autre côté, 90 % des Européens pensent qu'il est important de bénéficier des mêmes droits et de la même protection dans tous les pays de l'Union européenne.

La restauration de la confiance du public est donc nécessaire pour que les données personnelles puissent s'intégrer convenablement dans le « Marché unique numérique ». Mais face à une technologie mouvante et à l'émergence rapide de nouvelles techniques, une telle confiance ne peut naître dans l'esprit du public que si une certaine maîtrise de l'environnement numérique lui est donnée. La sensibilisation et l'éducation des utilisateurs à ces problématiques paraît donc un volet incontournable de la restauration de la confiance. Ce point n'a pas été ignoré par les institutions européennes qui commencent à bâtir une stratégie d'ensemble - basée sur une approche dite « relationniste » - en vue de construire une « culture numérique » accompagnant l'efficacité de la protection des données personnelles (§1). De la même manière, le développement et la sécurisation de l'identité électronique sera source de confiance pour le consommateur (§2).

[88] *Eurobarometer n° 431, « Data Protection », 2015*

§1. Eduquer le public à la protection des données personnelles : un nouveau défi pour les institutions européennes.

L'article 57 du RGPD reconnaît un rôle de sensibilisation et d'éducation du grand public dévolu aux autorités nationales de régulation. Cette mention explicite démontre la volonté des institutions européennes de permettre aux citoyens européens de retrouver une certaine confiance dans l'univers du numérique et de les accompagner dans la maîtrise de celui-ci. Cette logique est complémentaire aux dispositions législatives assurant la protection des données personnelles européennes. Il s'agit ainsi, en redonnant aux individus un pouvoir sur leurs données et en les sensibilisant aux problématiques en présence, de les accompagner dans leurs pratiques courantes, dans leur « vie numérique ». Les institutions européennes souhaitent donc permettre aux citoyens de créer et de partager leurs données personnelles en toute connaissance de cause, comme bon leur semble.

L'éducation au numérique constitue donc une priorité de la Commission européenne et des autorités de régulation des Etats membres. Tous estiment qu'une meilleure compréhension des mécanismes et du fonctionnement des services proposés par les acteurs du numérique permettra aux citoyens de faire usage de leurs données personnelles dans un climat de confiance, nécessaire à la croissance du secteur du numérique. La démarche pédagogique mise en œuvre pour ce faire démontre l'adoption d'une approche « relationniste » par l'ensemble des autorités de régulation européennes. Cette approche peut s'illustrer, en pratique, par la publication de supports d'enseignement par la CNIL (A). Toutefois, cette logique pédagogique ne semble pas être suffisante, comme l'illustrent les problèmes pouvant être posés par les conditions générales d'utilisation (B). Enfin, une solution censée donner aux individus la maîtrise absolue de leurs données personnelles est actuellement débattue par la doctrine : il s'agirait d'en faire un droit de propriété, en les considérant comme des biens comme les autres (C).

A. L'adoption d'une approche « relationniste » par la CNIL : l'exemple des supports d'enseignement.

De ce fait, la CNIL a créé des programmes d'information et de sensibilisation aux enjeux présentés par les données personnelles. Ces programmes sont des supports pédagogiques destinés à l'enseignement. Ils sont adaptés au niveau scolaire de leurs destinataires.

Ainsi, la CNIL a publié un guide destiné aux lycéens.[89] Elle y invite les enseignants à attirer l'attention des élèves sur la législation « informatique et libertés » et sur la nécessité de bien comprendre ce qu'englobe le terme de données à caractère personnel. Une approche plus pratique est également envisagée au travers de laquelle les élèves sont informés de leurs droits et des obligations incombant au responsable de traitement. Le guide traite également de thématiques touchant à la vie courante, plus proches de cette catégorie d'âge comme les données scolaires, la création de sites web, de blogs et bien-sûr, les réseaux sociaux.

De la même manière, la CNIL a développé un guide pour les études supérieures.[90] La logique de sensibilisation est, là encore, très marquée. Les thèmes abordés sont également adaptés aux préoccupations des étudiants, des chercheurs ou encore des Professeurs. Le guide traite ainsi, notamment, des modalités de traitement des données des étudiants (enquête statistiques, publication des résultats aux examens, mise à disposition de ressources numériques) ou encore des problématiques posées par les données personnelles dans le milieu professionnel (utilisation du téléphone portable sur le lieu de travail, de la messagerie électronique, etc.).

Outre le milieu de l'enseignement, la CNIL adopte également une démarche extrêmement pédagogique sur son site Internet. La clarté et l'abondance de son contenu permettent une meilleure visibilité du cadre légal « informatique et libertés » pour les professionnels du numérique. Le site web peut donc être un véritable guide pour les responsables de traitement. Mais celui-ci n'est pas seulement destiné aux professionnels, en effet, il explique également aux citoyens quels sont leurs droits face au traitement de leurs données personnelles et quelles sont les obligations des responsables de traitement. Il indique également de manière précise et dans des termes accessibles par tous, de quelle façon ils peuvent exercer leurs droits.

B. La lutte contre le dysfonctionnement informationnel : l'exemple des conditions générales d'utilisation.

Cependant, malgré le développement d'une certaine pédagogie, prônée par les institutions européennes et mise en œuvre par les autorités nationales, certains défis restent entiers en matière d'information et de sensibilisation des citoyens.

---

[89] *Guide CNIL « Informatique et libertés pour l'enseignement du second degré », édition 2010*

[90] *Guide CNIL, « Informatique et libertés pour l'enseignement supérieur et la recherche », édition 2011*

L’approche relationniste, seule, ne pouvant être suffisante pour y faire face, une action relativement « forte » et réfléchie du législateur semble alors nécessaire. Un exemple flagrant de dysfonctionnement de l’information du public réside dans les conditions générales de vente (CGV) ou d’utilisation (CGU). En effet, même sous couvert d’une gratuité apparente pouvant être très attrayante, la relation qui unit le responsable de traitement à son client reste une relation commerciale. Face aux pratiques, souvent trompeuses, de certains prestataires du numérique, l’encadrement juridique semble devoir être renforcé et adapté aux spécificités présentées par le secteur du numérique, droit de la consommation en première ligne.

On peut alors rappeler que le RGPD réaffirme l’obligation pour le responsable de traitement de recueillir un consentement libre et éclairé préalablement à la collecte ou au traitement de données personnelles. Cette obligation lui revient qu’il se trouve, ou non, dans un contexte de relations commerciales. Le consentement de l’utilisateur est révocable à tout moment. Dans le cadre de la collecte de données personnelles, l’« opt in » devient alors le principe et le consentement tacite, l’exception. Ce dernier reste possible mais dans des cas de figure limités (en cas d’obligation légale, ou pour préserver les intérêts de la personne concernée, par exemple). La simple mention d’un encadré indiquant que le site web consulté collecte des informations sur la navigation de l’internaute ne suffira donc, en principe, plus pour que le consentement soit légalement obtenu.

Cependant les CGU ne cesseront pas pour autant de présenter des risques pour la protection de la vie privée des internautes. En effet, il peut exister une forte pression à l’usage d’un service. Pression qui pourrait conduire l’individu à accepter les CGU bien qu’il les désapprouve. On peut alors prendre l’exemple de l’application « Pokémon Go » ou du réseau social Facebook, dans la cour de récréation d’un collège ; ou encore celui de l’usage de réseaux comme « LinkedIn » dans le milieu professionnel. D’autre part, les CGU peuvent être modifiées par le prestataire en cours de route. Ainsi, le réseau social Twitter a pu modifier, en 2009, les dispositions de ses CGU en matière de confidentialité pour revendre par la suite l’équivalent de deux années de publications à des entreprises de prospection de données. Enfin, malgré la proclamation de l’« opt in » comme solution de principe, la plupart des CGU n’en resteront pas moins longues, rébarbatives et très peu claires. On peut alors penser que le consentement sera bel et bien donné par l’utilisateur sans qu’il n’ait réellement conscience de ce que cela implique.

Une volonté de simplification commence alors à voir le jour. Cette simplification passerait, selon certains, par le recours à l'iconographie, qui serait commune à tous les acteurs du web. Des symboles traduiraient alors la politique du prestataire en matière de données personnelles, des modalités de leur collecte et de ce qu'il en adviendra par la suite (finalité du traitement, possibilité de revente à des tiers, transfert des données à l'étranger, etc.).

C. *La création d'un droit de propriété sur les données personnelles : une « fausse bonne idée » ?*

Une nouvelle approche de la protection des données personnelles est récemment apparue. Elle divise actuellement la doctrine. Il s'agirait de créer un droit de propriété de l'individu sur ses données personnelles. Celles-ci pourraient alors être comparées à une œuvre de l'esprit protégée par la Propriété intellectuelle ou à une marchandise négociable et cessible. Or, la monétisation d'informations personnelles se place grandement à contrecourant des visions françaises et européennes de la vie privée, droit fondamental de l'individu. Par ailleurs, mettre en place un tel système, en inscrivant les données personnelles dans le commerce juridique, reviendrait à « *renvoyer sur l'individu la responsabilité de gérer et de protéger ses données, au lieu de trouver des réponses collectives à un problème de société et participe d'une vision qui renforce l'individualisme et nie les rapports de force entre les consommateurs et les entreprises* ».[91] La possibilité d'une marchandisation de la vie privée ouvre la porte à des dérives conscientes et à des abus « légaux » de la part des entreprises du secteur privé.

En effet, il est clair qu'en utilisant des services numériques dans la vie courante, les individus se retrouvent souvent peu conscients des risques qui planent sur leurs libertés fondamentales. Pourtant, l'application d'une telle solution renverrait aux seuls individus - désarmés - la responsabilité de l'usage de leur données personnelles. En faire un élément patrimonial pourrait donc laisser place à une protection plus faible des citoyens. Effectivement, céder ses données à un tiers prestataire (Google, Facebook, Etat, etc.) reviendrait également à perdre les droits garantis par la loi. L'individu céderait alors ses données personnelles mais avec elles partiraient également son droit à l'oubli, son droit de rectification et de suppression.

[91] *Valérie Peugeot, « Données personnelles : sortir des injonctions contradictoires », Vecam. 13 avril 2014, voir http://vecam.org/Donnees-personnelles-sortir-des-injonctions-contradictoires.*

L'argument consistant à prétendre que les individus disposeraient d'une plus grande maîtrise de leur environnement numérique s'ils étaient propriétaires de leurs données personnelles semble donc erroné. Certes, ils jouiraient d'une liberté totale d'en disposer et d'en faire ce que bon leur semble, pouvant ainsi édifier eux-mêmes les barrières de leur vie privée. Mais il semble que leur liberté n'en serait que très relative puisqu'ils n'ont pas forcément conscience des implications de leurs choix. Pour une majorité de citoyens, instaurer un tel système sans avoir au préalable diffusé une certaine « culture numérique », reviendrait en quelques sortes à supprimer la protection de leurs données personnelles et des droits y étant attachés. Or, du fait du caractère intime de ces données et de leurs liens à l'individu, une telle perte pourrait bien s'apparenter à la perte d'une partie de soi-même.

§2. Le développement de l'identité numérique comme vecteur de confiance pour les citoyens européens.

La notion d'identité numérique peut être synonyme d'« e-réputation ». Elle désigne dans ce cas un ensemble d'informations divulguées par un individu sur le réseau et qui lui sont propres. Mais ce terme peut également se rapporter à l'identification d'un individu sur l'Internet. Il désigne alors un moyen de prouver son identité à distance, sur le web. L'identité numérique peut ainsi prendre la forme d'un mot de passe, d'une clé USB sécurisée, d'un smartphone, d'une carte électromagnétique, etc. Elle constitue à la fois un moyen d'accès sécurisé à des pages web, formulaires, services, ou autres, mais également une donnée personnelle en soi, revêtant une valeur juridique spécifique. La sécurisation et le développement de ces moyens de preuve de l'identité sont sources, pour le public, de confiance dans l'univers numérique. Le développement de l'identité numérique et son harmonisation sur le territoire de l'Union européenne s'inscrit donc pleinement dans le cadre de la construction du « Marché unique numérique » et du développement des échanges dématérialisés.

Sur l'Internet - pourtant accessible à tous et de manière anonyme - l'identification de l'individu peut être rendue nécessaire pour, par exemple, pouvoir accéder à des dossiers personnels (qu'ils soient d'ordre médical, administratif, professionnel ou simplement personnel). Pendant longtemps, il n'existait pas, en droit européen, de moyens juridiques de prouver son identité en ligne. Cette possibilité devait être définie contractuellement, comme c'est le cas pour les cartes bancaires.

Aujourd'hui, des cartes d'identité électroniques sont délivrées par de nombreux pays européens et permettent de s'identifier sur le web grâce à des lecteurs incorporés aux ordinateurs. Par ailleurs, le règlement européen du 23 juillet 2014, dit « elDAS »[92] (entré en vigueur le 1er juillet 2016) reconnaît certains services d'identification à distance comme la signature électronique des personnes physiques ou morales, l'envoi électronique d'un recommandé, l'authentification d'un site web, etc. Il harmonise les règles et les modalités de reconnaissance de ces techniques d'identification. Ce faisant, il organise alors la création d'une « identité numérique » européenne. Une telle entreprise est louable puisqu'elle permettra de favoriser le commerce électronique et les échanges intra-européens recourant à l'Internet.

Ainsi, les Etats ne sont pas les seuls à pouvoir offrir aux individus des moyens de prouver leur identité. Des organismes privés sont également en capacité de le faire sur des supports variés. Ces modes d'identification sont de plus en plus adaptés à l'usage concret qu'on l'on peut avoir de l'Internet. En effet, de nos jours, la connexion suit les usagers partout où ils vont. Ainsi, les grandes entreprises du numérique y voient une opportunité commerciale et commencent à exploiter ce filon. Elles commencent à développer de nombreuses techniques permettant à l'internaute de s'identifier sur le web, avec plus ou moins de fiabilité. Elles peuvent ensuite revendre ces services d'identification à des tiers. On peut ainsi prendre l'exemple du formulaire Facebook (« Facebook login ») où la page Facebook d'un individu est censée attester de son identité. Cette identité numérique est présente sur des millions de sites web à travers le monde. Toutefois, la remise en question de la fiabilité de ce procédé paraît évidente puisqu'il est possible de créer un faux compte Facebook, avec de faux identifiants, etc. On peut également citer le formulaire PayPal, qui lie un compte utilisateur a un compte bancaire. Ce qui est de nature à accroitre la crédibilité de l'identification. Cette technique a d'ailleurs été homologuée de manière officielle par l'administration britannique.

Face à la sécurisation de ces données personnelles, le règlement « elDAS » n'est pas resté muet. En effet, le recours à l'identification électronique n'est pas sans conséquence sur la confiance que portent les citoyens dans le commerce électronique ou plus généralement dans l'univers numérique.

[92] *Règlement (UE) n ° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*

Pour compulser les échanges et donc le développement économique en Europe, le règlement souhaite rendre le document électronique juridiquement équivalent à un document papier. Il met alors en place plusieurs niveaux de sécurité : un dit « faible » (présentant un « degré limité de fiabilité »), un autre dit « substantiel » et enfin un niveau dit « élevé » pour lequel les risques d'usurpation ou de piratage sont considérablement réduits. Celui-ci disposera d'une valeur juridique supérieure, équivalente aux documents d'identification « traditionnels ».

Le règlement prévoit également que les services administratifs des Etats membres s'adaptent à ces nouvelles formes d'identification des administrés. Ils auront ainsi l'obligation d'accepter les moyens d'identification en provenance d'autres Etats membres lorsque ceux-ci assureront un niveau de protection équivalent aux procédés qu'ils ont l'habitude d'utiliser. Ils devront alors mettre en place les dispositifs techniques nécessaires à l'utilisation de ces nouvelles identités numériques. Par ailleurs, la Commission européenne dresse une liste des systèmes présentant un niveau de sécurité élevé. Une présomption de sécurité sera alors établie si le moyen d'identification respecte des normes techniques mises en place par la Commission. Les Etats membres devront alors reconnaître des identités numériques sécurisées émises dans tout le territoire européen. Ces identités pourront aussi bien s'appliquer à des personnes physiques qu'à des personnes morales.[93]

Ces dispositions favorisent l'émergence de nouveaux moyens d'identification numérique, se substituant à la carte d'identité, au passeport, ou à d'autres moyens « classiques » de certifier l'identité. Ces nouvelles identités numériques paraissent plus pratiques et seront surement, dans l'avenir, plus sécurisées (plus de perte ou de vols de papiers d'identité, réduction des possibilités d'usurpation de l'identité sur Internet, etc.).

Cette identité numérique est elle-même, quelque part, le spectre de la construction d'une véritable « identité mondiale » - tout du moins européenne - affranchie de toute frontière étatique et de toute Nationalité. Ainsi, Google a annoncé travailler à la distribution, dans le monde entier, de certificats d'identité électroniques délivrés sur clés USB, ce qui serait concrètement le premier pas d'un service d'identité mondial.

[93] *Fabrice Mattatia, « Le droit des données personnelles », Eyrolles 2ème édition, 2015, page 100*

II. Promouvoir la circulation des données personnelles tout en responsabilisant les opérateurs du numérique.

Dans le cadre de la lutte contre les difficultés engendrées par l'émergence des technologies numériques, les institutions européennes ont décidé d'agir sur l'utilisateur, de l'éduquer et de lui redonner confiance dans le secteur du numérique. Mais elles ont également pris conscience de la possibilité d'agir directement sur les opérateurs économiques, de développer un cadre de corégulation. Ce qui reviendrait à les pousser à s'impliquer davantage dans la protection des données personnelles. Les entreprises peuvent également prendre conscience d'elles-mêmes de l'importance de développer et de limiter de tels outils puisqu'elles ont tout intérêt à conserver la confiance de leurs clients. Il s'agit alors pour les institutions européennes de faire de cette confiance un aspect significatif de la compétitivité et de différenciation des opérateurs du numérique. La régulation mise en œuvre serait alors appliquée au mieux par les professionnels eux-mêmes. Elle serait même complétée par des initiatives privées relevant de l'autorégulation. Au-delà d'une logique de « responsabilisation » des opérateurs du numérique (« accountability ») (§1), ces derniers sont amenés à participer d'eux-mêmes à la protection des libertés fondamentales des citoyens européens, celle-ci étant devenue un vecteur de compétitivité et de différenciation (§2).

§1. L'émergence de l' « accountability » : la responsabilisation des opérateurs du numérique et la recherche d'une corégulation.

Initialement, le terme d' « accountability » se réfère à l'obligation du mandataire de rendre des comptes à ses mandants. En matière de protection des données personnelles, l' « accountability » désigne des systèmes de gouvernance de la conformité internes aux entreprises. Dès 1991, le gouvernement américain a pris un décret[94] instaurant des sanctions relativement lourdes pour les opérateurs du numérique méconnaissant les principes de la protection des données.

[94] *US Sentencing Commission Guidelines, Sentencing for Organizations, 56 Fed. Reg. 22,762 (1991)*

Il cherchait par là à inciter les entreprises à adopter des politiques internes en matière de conformité dans de très nombreux domaines (données personnelles mais aussi environnement, comptabilité, concurrence, etc.). Le décret prévoit que ces sanctions soient atténuées dans le cas où les opérateurs auraient mis en place un système d'autorégulation. Ceci a eu pour effet de développer de manière significative les démarches de responsabilisation des entreprises américaines. Au fil du temps, la participation des entreprises au processus de régulation s'est développée. Cette logique de corégulation a été reprise par les institutions européennes, qui l'ont intégrée dans le règlement du 27 avril 2016 (article 5). Il s'agit là d'une des révolutions majeures apportées à la protection européenne des données personnelles. De la même manière qu'aux Etats-Unis, les procédures d' « accountability » mises en place par les opérateurs du numérique seront prises en compte dans la détermination des sanctions pouvant leur être infligées par les autorités de régulation.

Le responsable de traitement doit ainsi participer de manière active à la protection des données personnelles : il doit mettre en place un cadre contraignant qui lui est propre, adapté à ses activités. Il devra également mettre en place une « culture éthique » en sensibilisant ses salariés (par des « formations informatique et libertés », par exemple), ainsi que des mécanismes visant à révéler les non conformités éventuelles (audit, ou système d'alerte interne, dit « Whistleblowing », par exemple). La preuve par l'entreprise de sa conformité en matière de protection des données lui permettra de (re)gagner la confiance de ses clients et sera un moyen de valoriser les dispositifs mis en place. Ainsi, le responsable de traitement aura la possibilité de véhiculer une image positive auprès du public. Il s'agit là d'un « enjeu de crédibilité » et de différenciation pour les acteurs du numérique. Naturellement, la coopération entre le régulateur et les professionnels du secteur du numérique n'implique pas la substitution du secteur privé au rôle du législateur ou des autorités publiques. L'autorégulation doit aller de pair avec la régulation, l'accompagner, l'approfondir. Il s'agit en réalité d'un usage professionnel qui complète les normes législatives et règlementaires. Au fil du temps, de tels usages permettront aux dispositions légales de perdurer et de s'adapter aux évolutions technologiques. Il s'agit donc d'un outil d'anticipation dans un univers évoluant à une vitesse considérable.

Si le règlement du 27 avril 2016 opère une réduction drastique des formalités administratives devant être remplies par le responsable de traitement, il lui impose tout de même l'obligation de prouver la conformité de ses pratiques aux dispositions législatives : il s'agit là d'une sorte de « contrat de confiance » (A).

Mais cette confiance ne doit pas relever de la naïveté : des contrôles a posteriori ont été prévus par le législateur et planent sur les opérateurs du numérique. Ces derniers disposent alors de certains outils pour démontrer la conformité de leurs agissements (B).

A. *La réduction des charges administratives : l'introduction d'un « contrat de confiance » avec les acteurs du numérique.*

La Directive de 1995 avait principalement fondé la régulation de la protection des données sur un contrôle a priori exercé par les autorités nationales par le biais de formalités préalables au traitement. Cette logique a été reprise par le législateur français qui l'a transposée dans la loi « Informatique et libertés », comme nous avons eu l'occasion de l'étudier plus en avant[95]. Or, une telle approche a pu connaître quelques limites de taille. D'abord, un paradoxe quantitatif : la CNIL s'est vue engorgée de déclarations préalables et de demandes d'autorisation alors qu'en réalité, très peu de responsables de traitement remplissaient les formalités légales exigées. Ensuite, une limite « matérielle » : la CNIL ne peut pas connaître la réalité des conditions du traitement par la simple analyse des formalités préalables, d'autant plus que celles-ci peuvent être erronées ou frauduleuses. Enfin, une limite « d'appropriation »[96] : les responsables de traitement, une fois les formalités préalables remplies, pouvaient avoir, à tort, le sentiment d'en avoir fini avec la problématique de la protection des données personnelles. Cela ne les encourageait pas à mettre en place une véritable gouvernance en la matière, ni à s'assurer du respect des dispositions légales sur l'ensemble de la durée du traitement.

Pour sa part, le règlement du 27 avril 2016 renverse totalement cette logique en appliquant celle de l'autorégulation ou « accountability » consistant à réduire les charges administratives de manière drastique tout en « responsabilisant » les opérateurs du numérique. Conformément à l'article 24 du RGPD, ceux-ci devront alors être en capacité de démontrer qu'ils assurent bien le niveau de protection des données fixé par le règlement. Celui-ci axe l'action des autorités nationales autour d'un contrôle a posteriori, laissant ainsi aux responsables de traitement la charge de s'autoévaluer.

---

[95] *Voir : Chapitre 2, Section 1, §1 : « Les formalités préalables devant être remplies par les responsables de traitement ».*

[96] *Stéphane Grumbach, « Données personnelles : ce que le règlement va changer pour les entreprises », Expertises des systèmes d'information, juillet 2013, page 253*

Dorénavant, l'opérateur devra effectuer un travail de qualification des données collectées et évaluer les risques que présente le traitement envisagé pour les libertés fondamentales des personnes concernées. Il devra alors en tirer les conséquences afin d'évaluer le régime juridique applicable et mettre en place, en interne, des mesures adaptées. Les responsables de traitement auront alors l'obligation de rendre des comptes, de démontrer la conformité de leurs pratiques et d'intégrer la régulation dans leur organisation interne. Ce qui suscite une certaine inquiétude dans le milieu du numérique car les formalités préalables restaient malgré tout un bon moyen de s'assurer de la licéité, sur le plan technique, des modalités du traitement. Ainsi, bien que les formalités préalables soient pour partie supprimées, le responsable de traitement doit néanmoins s'assurer de bien se conformer aux exigences légales.

Le RGPD introduit ainsi une approche basée sur le risque dans cette logique d'autoévaluation. En effet, plus le traitement présentera un danger pour les libertés fondamentales des citoyens européens, plus les précautions à prendre seront importantes. Il s'agira alors pour le responsable de traitement d'avoir recours à des outils de prévention et d'opérer en toute transparence pour faciliter le travail de contrôle des autorités nationales de régulation. On peut même observer le retour d'un certain formalisme préalable pour les traitements les plus « dangereux ».

B. Les outils mis à la disposition du responsable de traitement pour assurer la preuve de la conformité de ses agissements.

Comme nous venons de le voir, les formalités administratives sont quasiment abolies par le RGPD. Elles sont remplacées par des procédures internes que le CPO aura pour charge de superviser et de contrôler.[97]. Le responsable de traitement devra toutefois être en capacité de démontrer la conformité de ses pratiques en cas de contrôle des autorités nationales.

Pour ce faire, le RGPD lui impose la tenue d'une documentation sur les traitements mis en œuvre (1) ainsi que la réalisation d'une étude d'impact lorsque les circonstances entourant le traitement la rendront nécessaire (2).

[97] *Nathalie Mettalinos, « Données personnelles : vers une responsabilisation des entreprises », Expertises des systèmes d'information, mai 2014, page 174*

1) L'obligation de tenir une documentation détaillée sur les traitements.

Pour pouvoir s'assurer du respect par les opérateurs du numérique des dispositions légales en matière de protection des données et pour favoriser les contrôles a posteriori réalisés par les autorités nationales, le règlement oblige le responsable de traitement et ses sous-traitants à tenir une documentation rigoureuse. Celle-ci devra ainsi comporter de nombreuses informations sur le traitement mis en œuvre : finalité ; catégories de personnes visées ; données concernées ; destinataires des données personnelles recueillies ; transfert hors UE envisagé, le cas échéant ; etc. Ces informations sont similaires à celles qui devaient être fournies lors de l'accomplissement des formalités préalables prévues par la loi Informatique et libertés (donc à celles devant être transmises à la CNIL dans le cadre d'une procédure de déclaration ou d'autorisation). La charge administrative est donc considérablement allégée pour les seules autorités de régulation et non pour les responsables de traitement. En réalité, la charge et la gestion documentaire est transférée à ces derniers, qui doivent alors s'organiser en conséquence.

2) L'obligation de procéder à une étude d'impact en présence de traitements « à risque ».

L'article 35 du RGPD oblige le responsable de traitement à réaliser une étude d'impact ou « Privacy impact assessment » (PIA) lorsque le traitement envisagé comporte certains risques pour les personnes concernées, « *compte tenu de la nature, de la portée, du contexte et des finalités du traitement* ». L'article indique également que l'opérateur doit prendre en compte le « *recours à de nouvelles technologies* » lors de l'évaluation des risques. Ce qui place dans le dispositif un certain flou juridique volontaire. Il s'agit de se prémunir contre certains traitements qui pourront être mis en œuvre dans l'avenir à l'aide d'un procédé encore inconnu à l'heure actuelle. Cette disposition prévoyante permet ainsi d'anticiper une technologie qui pourrait se révéler particulièrement dangereuse pour les libertés fondamentales des citoyens européens. L'article 35 du règlement dresse ensuite une liste de traitements à risque pour lesquels une étude d'impact doit être menée de manière systématique. La liste, exhaustive en l'absence de formule telle que « notamment » (qui aurait été souhaitable), comporte les évaluations « *systématiques et approfondies (…) fondées sur un système automatisé* » d'éléments liés à la personnalité des individus (comme leur localisation, leur situation économique ou sociale, etc.) ; ainsi que le traitement de données de santé, génétiques, biométriques, attrayant à la sexualité, à l'origine

ethnique ou raciale ; ou encore les réseaux de surveillance publique (vidéo-surveillance). On pourra reprocher à cette liste d'omettre certains traitements qui pourraient pourtant induire des risques certains pour les libertés des personnes concernées comme ceux portant sur des données dites « sensibles » au sens de l'article 8 de la loi « Informatique et libertés » et relatives à l'orientation politique, à la religion ou encore à l'appartenance syndicale. Cependant, on peut répondre à cela que le règlement laisse la possibilité aux autorités nationales de dresser des listes de traitements particuliers devant faire l'objet d'une étude d'impact de manière systématique. L'article 35 précise encore les éléments qui doivent être présentés dans l'étude d'impact. Il indique ainsi que celle-ci « *contient au moins* » : une description des opérations nécessaires au traitement et la finalité de celui-ci ; une évaluation de la proportionnalité des moyens mis en œuvre au regard de la finalité déterminée ; une analyse des risques pour les droits des personnes concernées ; ainsi que les mesures envisagées pour préserver ces droits. Enfin, l'étude d'impact doit également faire état des « *garanties, techniques et mesures de sécurité* » adoptées par les entreprises pour assurer la protection des données personnelles.

Il est également prévu que le responsable de traitement recueille l'avis des personnes concernées au sujet du traitement envisagé. Cette dernière obligation pourra soulever des difficultés pratiques - voire s'avérer impossible à mettre en œuvre - lorsque le traitement concernera la surveillance de zones publiques ayant recours à des systèmes de vidéo-surveillance à grande échelle. En effet, il est inimaginable de recueillir l'avis de toutes les personnes filmées dans une ville, ou simplement dans une rue. Cela pourrait également réduire la pertinence ou l'efficacité de tels dispositifs. Cette problématique ressurgira également en présence de traitements à grande échelle, de profilage notamment.

Pour finir, il semble opportun de noter ce que l'on pourrait interpréter comme le retour d'une des formalités préalables les plus lourdes organisées par la loi Informatique et libertés : la procédure d'autorisation. En effet, le règlement prévoit que lorsque l'étude d'impact démontrera un « degré élevé de risques particuliers », le responsable de traitement devra consulter l'autorité de contrôle compétente. Il s'agit là d'un des rares cas de figure dans lequel une formalité préalable est maintenue. Dans cette hypothèse, l'autorité de contrôle compétente devra indiquer au responsable de traitement les mesures à adopter dans un délai de 2 mois. Elle pourra également interdire le traitement ou enjoindre le responsable de traitement à mettre en place des mesures de mise en conformité.

§2. L'émergence d'autres outils d'autorégulation comme vecteurs de compétitivité et de différenciation pour les professionnels du numérique.

L'autorégulation recherchée par les institutions européennes obéit à une logique de prévention : il s'agit de pousser les entreprises à développer d'elles-mêmes des moyens de protection des données personnelles de leurs clients. Transformer l'autorégulation en une forme de « course à la compétitivité » permettrait d'augmenter de manière considérable le niveau de protection des données des citoyens européens. Cela permettrait également de prévenir l'obsolescence des dispositions législatives face à la rapidité des avancées technologiques dans le domaine du numérique. Outre leur responsabilisation, les responsables de traitement se voient donc amenés à participer au processus de régulation, que ce soit dès la conception d'un produit ou service « Privacy by design » (1) ou par la possibilité d'obtenir des certifications (2). Ces outils leur permettront de se différencier sur le marché et d'attirer un public toujours plus friand de garanties quant à la protection de sa vie privée.

A. L'autorégulation par la protection de la vie privée dès la conception.

La régulation de l'usage des données personnelles peut très vite se retrouver dépassée. L'autorégulation peut alors s'y substituer et permettre de l'adapter aux évolutions technologiques. Les entreprises doivent alors trouver comment concilier protection des utilisateurs et innovation sachant que les nouvelles techniques numériques (Big Data et géolocalisation en première ligne) s'opposent souvent au respect de leurs libertés fondamentales. Elles doivent alors mettre en place une solution compromissoire, leur permettant d'être gagnantes à tous les niveaux. Ainsi, le « Privacy by design » où protection de la vie privée dès la conception est prévu par l'article 25 du RGPD. Cette technique a vocation à gérer et à aider les individus à contrôler plus aisément la divulgation de leurs données personnelles. Le responsable de traitement peut alors intégrer directement dans les biens ou services qu'il commercialise des systèmes permettant, par exemple, de rendre les données collectées anonymes ou d'autres permettant aux utilisateurs de maîtriser la diffusion de leurs données personnelles. De ce fait, l'opérateur est non seulement respectueux de la réglementation et des droits de ses utilisateurs, mais il peut également profiter des avantages du Big Data.

Par exemple, Microsoft a doté son navigateur web, « Internet Explorer », de la fonction « do not track by default ». Apple en a fait de même sur son navigateur web, « Safari » et Google sur son navigateur, « Chrome ». L'utilisateur peut ainsi choisir d'activer l'option « navigation privée » permettant de rendre leurs recherches « invisibles ». Les moteurs de recherche ont également très vite compris la nécessité de mettre en place de tels outils, certains en ont même fait leur spécialité. C'est le cas du moteur de recherche « Duck Duck Go » dont le slogan est : « le moteur de recherche qui ne vous espionne pas ». Il est apprécié par de nombreux internautes car il ne collecte - et donc ne partage - aucune information sur les recherches (adresse IP, trace numérique, etc.). Selon les études du cabinet Alexa[98], le trafic généré par le moteur de recherche « Duck Duck Go » est en très forte évolution depuis l'affaire PRISM.

Résultant d'une approche pluridisciplinaire - alliant le travail de juristes, d'ingénieurs et de représentants du responsable de traitement - le « Privacy by design » marque une certaine complémentarité entre la loi et la technologie. Mais cette pratique est encore très peu développée. On peut anticiper une prise de conscience de la part des GAFA notamment, sur l'importance de cette relation et prévoir ainsi une forte augmentation de l'autorégulation du secteur du numérique dans les années à venir.

B. L'autorégulation par l'attrait de la certification.

L'article 11 de la loi « Informatique et libertés » prévoit que la CNIL puisse décerner des labels à « *des produits ou des procédures tendant à la protection des personnes à l'égard du traitement des données* ». Elle publie ainsi des références auxquelles les acteurs du numérique doivent se plier pour obtenir une labellisation. Le fait de bénéficier d'une certification permet aux entreprises d'acquérir une certaine attractivité et de se différencier de la concurrence. Cela permet donc d'inciter les entreprises à se lancer dans une « course à l'éthique ». La certification est un moyen très efficace de « fidéliser » le secteur privé à l'autorégulation et d'augmenter la transparence des acteurs du numérique. C'est également un moyen pour eux de valoriser leur « capital confiance », d'en tirer le meilleur parti, en voyant leurs bonnes pratiques portées aux yeux de tous.

[98] *Le cabinet Alexa Internet, fondé en avril 1996 à San Francisco est une filiale du groupe Amazon réalisant des statistiques sur le trafic web mondial*

Un label se construit sur une double base par les autorités de régulation. Tout d'abord, par l'établissement d'un référentiel commun (niveau de protection des données sensibles ; durée de conservation des données ; politique en matière de transfert ; chiffrement ; etc.) permettant aux prétendants d'analyser la conformité de leurs pratiques au niveau d'exigence requis. Il passe ensuite par la mise en œuvre de contrôles effectifs permettant de vérifier la bonne application des engagements pris par les responsables de traitement ayant obtenu la certification. Il ne s'agit pas de labéliser l'entreprise sur une situation donnée à un instant « t » mais de suivre son évolution et de s'assurer qu'elle respecte bien les normes imposées au fil du temps.

Jusqu'à aujourd'hui, la CNIL a créé quatre labels : un relatif aux procédures d'audits des traitements, dit « procédure d'audit » ; un autre consacré aux formations informatiques et libertés du personnel, dit « formation » ; un concernant les « coffres-forts » numériques ; et enfin, un label attestant de la « gouvernance informatique et liberté » de l'entreprise. Ce dernier a été créé en novembre 2015 et a vocation à aider les responsables de traitement à identifier les mesures à mettre en place pour assurer une bonne gestion des données personnelles. Le label « gouvernance informatique et libertés » gravite autour de trois axes : l'organisation interne, les méthodes de vérification de la conformité aux dispositions légales et la gestion des réclamations et des incidents.

Si l'actuel Projet de loi « pour une République numérique » renforce les pouvoirs de labellisation de la CNIL en vue de la création d'une certification relative à l'anonymisation des données personnelles (notamment dans le cadre de l'Open data), le législateur européen n'est pas resté muet face au mécanisme de certification. Ainsi, deux articles du RGPD y sont consacrés : les articles 39 et 39 bis. Le terme même de certification, absent dans la directive de 1995, y est ainsi consacré. La certification a désormais vocation à s'appliquer aux responsables de traitement ainsi qu'à leurs sous-traitants, que ceux-ci soient européens ou non, donc visés par les dispositions du RGPD ou non. Le fait que la certification ne se réduise pas aux seuls acteurs auxquels le règlement est opposable permettra de faciliter le transfert international de données personnelles. En effet, cela va inciter de nombreux opérateurs non européens à s'engager dans un mécanisme de certification pour pouvoir attester d'un niveau suffisant de protection auprès des autorités de régulation européennes.

Par ailleurs, durant les deux années à venir, jusqu'à l'entrée en vigueur du RGPD, les autorités nationales de régulation vont devoir opérer un travail collectif conséquent pour construire une véritable politique européenne de la certification. En effet, les certifications de chaque Etat membre devraient être relativement proches pour que le citoyen européen puisse s'y retrouver dans le cadre intracommunautaire. Ainsi, les pouvoirs d'autorisation des autorités nationales ont été encadrés et normalisés par le règlement. Ils s'articulent autour de critères communs pour assurer une certaine cohérence dans les processus de certification. Ces critères sont, par exemple, l'indépendance, le degré d'expertise, l'absence de conflit d'intérêt de l'organisme de certification, l'examen périodique des organismes certifiés, la durée de la certification (qui est de 3 ans) ou les modalités de son retrait, etc. Ils permettent d'assurer « *l'évolution du modèle actuel de la certification vers une posture interventionniste visant à écarter l'influence des organismes de certification insuffisamment compétents, indépendants ou impartiaux (...)* ».[99]

Suivant la même logique d'uniformisation des certifications dans le « Marché unique numérique », l'introduction d'une certification européenne dans le domaine de la donnée personnelle est envisagée par le G-29 pour la fin de l'année 2016.

Pour inciter les acteurs du numérique à mettre en place des mesures techniques de protection des données personnelles, on peut aisément imaginer une labellisation « Privacy by Design ». Ni les autorités de régulation, ni même les opérateurs du numérique ne disposent actuellement d'un recul suffisant sur les nouvelles technologies pour pouvoir établir des référentiels communs. Mais des recommandations générales pourraient permettre de prévoir des moyens techniques ou des modes d'organisation permettant le respect de la vie privée et des droits des utilisateurs. De telles recommandations générales, auraient, certes, moins d'efficacité, mais auraient tout de même le mérite d'exister et de guider les futurs CPO dans leur mission d'accompagnement des nouveaux projets.

[99] *Olivia TAMBOU, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », Revue Lamy de Droit de l'Immatériel, avril 2016, p. 51*

Chapitre 2 : La régulation du transfert de données personnelles en dehors de l'Union européenne.

Au fil du temps, le contexte de globalisation ne va pas en s'amenuisant. Le développement d'Internet induit sans cesse une dématérialisation des frontières pour des échanges internationaux de plus en plus conséquents. Plus globalement, l'ensemble du secteur du numérique est lui-même soumis au phénomène de mondialisation. Engagés dans une véritable guerre concurrentielle et pressés par les attentes croissantes de rentabilité de leurs actionnaires, ses acteurs sont prédisposés à avoir recours à l'externalisation informatique. Ils sont alors amenés à se tourner vers des Etats qui présentent de faibles coûts de main d'œuvre (par exemple pour la construction d'infrastructures de stockage de données ou pour la prestation de services numériques, comme le service après-vente, la gestion de la paye, la hotline client, etc.), ainsi que de faibles taux d'imposition ...

Mais cette tendance à la délocalisation peut également s'expliquer par le fait que les responsables de traitement de données à caractère personnel recherchent des systèmes juridiques peu engagés dans la protection des données, de manière à pouvoir opérer de manière plus libre, avec le minimum de restriction possible. Par conséquent, les demandes d'autorisation pour les transferts internationaux de données personnelles ne cessent de croître.

Ce phénomène est également accentué par l'émergence du « Cloud computing », terme qui désigne une méthode d'externalisation des serveurs de stockage de données. C'est un procédé par lequel un organisme détenteur de données fait appel à des serveurs qui lui sont extérieurs. Ces serveurs, d'une capacité et d'une taille considérable, sont gérés par des géants comme Google, Microsoft ou par des entreprises moins connues des autorités de régulation. Ils sont répartis dans le monde entier et sont interconnectés. De cette manière, il devient presque impossible de savoir où se trouve concrètement la donnée à un instant « t ». Se pose alors le problème de savoir quel droit compétent aura vocation à la protéger. Ainsi, la régulation de l'exportation de la donnée devient, elle aussi, quasiment impossible. Pour corser cette difficulté, la donnée peut également être fractionnée et répartie dans le cloud, donc dans le monde entier. La donnée en elle-même est alors partout et nulle part à la fois.

Sur le territoire européen, la Directive européenne de 1995 a permis de prodiguer un niveau de protection équivalent dans chaque Etat membre. Ce qui a eu pour effet de dispenser les transferts de données limités au territoire de l'Union de toute formalité administrative. Une telle exemption a conduit à y faciliter les transferts de données, permettant une libre circulation de l'information à travers l'ensemble du territoire. Toutefois, le phénomène de l'externalisation informatique s'applique également aux opérateurs européens. Ainsi, les échanges de données ne cessent d'augmenter entre filiales d'une multinationale, entre entreprises distinctes (recours à des sous-traitants extérieurs à l'Union) ou entre internautes européens et opérateurs du numérique basés en dehors du territoire européen. Les données européennes sont donc constamment amenées à voyager et cette tendance est en hausse. Mais les pays dans lesquels elles circulent ne sont pas toujours respectueux des droits et libertés des citoyens européens et aucun instrument juridique international n'assure leur protection de manière effective.

Les institutions européennes limitent alors la possibilité de transférer des données hors de l'Union à l'assurance que celles-ci sont au moins aussi bien protégées que sur le territoire européen (I). Ces limitations « de droit commun » connaissent une dérogation de taille dégagée autour de négociations s'inscrivant dans le cadre des relations commerciales qu'entretient l'Union européenne avec les Etats-Unis : le tout nouveau « Privacy Shield » remplaçant feu le « Safe Harbor » (II).

I. Le « droit commun » de l'exportation des données personnelles : la recherche d'une protection territoriale « adéquate ».

Dans le but d'assurer l'application des principes fondamentaux assurant la protection des données personnelles des citoyens européens au cours d'éventuels transferts en dehors du territoire de l'Union, le droit européen et le droit national exigent un niveau élevé de protection des données exportées. Si l'adéquation de la protection est en principe reconnue par décision de la Commission européenne (§1), elle peut également être matérialisée, dans certaines circonstances, en l'absence d'une telle décision (§2). En dehors de telles hypothèses, le transfert de données personnelles hors de l'Union européenne est considéré comme illicite et expose son auteur à se voir appliquer l'article 226-22-1 du Code pénal. Celui-ci dispose que « *le fait, hors les cas prévus par loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartement pas à la communauté européenne (…)* » est sanctionné de 300.000€ d'amende et de 5 ans d'emprisonnement, l'amende pouvant être portée à 1.500.000€ si le transfert est réalisé par une personne morale. Contrairement aux autres infractions pénales en matière de données personnelles, celle-ci peut être commise par le responsable de traitement lui-même, mais également par celui qui « fait procéder » au transfert. Cependant, les condamnations pénales sur ce fondement sont rares.

§1. La licéité des transferts reconnue par décision d'adéquation de la Commission européenne.

L'exportation de données personnelles vers un pays tiers n'est en principe autorisée que si ce pays assure un niveau de protection des données adéquat. L'adéquation de la protection fournie par un Etat tiers est mesurée par la Commission européenne. Aux termes de l'article 25 de la directive de 1995, le caractère adéquat de la protection s'analyse au regard de « *la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées* ».

La Commission doit donc rechercher si le système national de protection des données personnelles du pays ciblé est semblable à celui qu'assure le droit européen. L'adéquation ne s'analyse donc pas comme une équivalence entre les deux systèmes mais, de manière globale, comme l'apport de garanties suffisantes quant au respect des droits et libertés des citoyens européens. Peu importe si les moyens auxquels l'État tiers a recours pour assurer une protection adéquate sont différents de ceux habituellement utilisés au sein de l'Union européenne.[100] La Commission doit ainsi vérifier le contenu des règles applicables autant que leur mise en œuvre et leur effectivité.

Avec le RGPD, le législateur européen est venu préciser les conditions de l'adéquation. En effet, celui-ci dresse une liste des critères d'adéquation à son article 45. On peut alors retrouver : « *l'état de droit, le respect des droits de l'homme, (…) les règles en matière de protection des données, (…) les règles professionnelles et les mesures de sécurité, (…) les droits effectifs et opposables dont bénéficient les personnes concernées, (…) les engagements internationaux pris par le pays tiers* », etc. Il s'agit donc pour la Commission de vérifier que l'Etat tiers respecte les droits fondamentaux accordés aux personnes concernées, qu'il assure une limitation effective de la réutilisation des données, qu'il y existe une autorité de contrôle indépendante et que les citoyens européens disposent bien d'une voie de recours en cas de manquement de la part du responsable de traitement ou de contestation des décisions rendues par les autorités administratives. Le pouvoir d'appréciation de la Commission est donc dorénavant encore plus limité qu'il n'a pu l'être du fait de la jurisprudence de la Cour de justice. En effet, celle-ci l'encadrait déjà de manière active, indiquant que « *le pouvoir d'appréciation de la Commission quant au caractère adéquat du niveau de protection assuré par un pays tiers s'avère réduit, de sorte qu'il convient de procéder à un contrôle strict des exigences découlant de l'article 25 de la directive 95/46/CE, lu à la lumière de la Charte (européenne des droits fondamentaux)* ».[101]

Il incombe alors à la Commission européenne de dresser une liste d'Etats hors Union assurant ou non le niveau de protection adéquat. Cette liste peut être amenée à être révisée en cas de modifications positives ou négatives de la législation des Etats tiers. La décision d'adéquation de la Commission doit ainsi être revue au moins tous les quatre ans. On peut retrouver parmi

[100] *Romain PERRAY, « Arrêt Schrems : Cour(s) magistral(e) de droit à la protection des données, personnelles, Communication Commerce électronique n° 12, Décembre 2015, étude 21*

[101] *arrêt CJUE, 8 avril 2014, n° C-293/12, dit « Digital Rights Ireland »*

les Etats qui assurent un niveau de protection adéquat : le Canada, la Suisse, le Liechtenstein, le Royaume-Uni, l'Argentine, l'Uruguay, l'Israël, l'Australie et la Nouvelle-Zélande. Naturellement, les Etats de l'UE assurent une protection équivalente puisqu'ils ont tous été amenés à transposer la directive de 1995 dans leurs droits nationaux. A fortiori, ils se verront tous appliquer une régulation uniforme dès lors que le règlement du 27 avril 2016 sera entré en vigueur.

D'autre part, du fait de l'absence de frontières sur l'Internet, les informations véhiculées par des sites web peuvent traverser le monde et être captées par des responsables de traitement situés dans des Etats n'assurant pas la protection adéquate requise par les textes. Il a donc fallu se demander si la notion de « transfert » pouvait s'appliquer en de pareilles circonstances. Cette problématique est fondamentale car, en l'absence de moyens de régulation des flux d'information sur le réseau, elle conditionne l'activité des sites web européens. La Cour de justice des Communautés européennes y a répondu par la négative, en indiquant qu'un site web implanté sur le territoire européen ne transfère pas de données personnelles dans des pays tiers, même si celles-ci sont accessibles dans le monde entier.[102] Bien que cette position puisse paraître critiquable sur le fondement juridique, elle se justifie largement par la réalité technique car il est impossible de contrôler la diffusion et l'accès aux informations présentes sur le web dans les Etats tiers. Une solution inverse aurait conduit les éditeurs web européens dans une position très délicate puisqu'ils auraient dû attendre que tous les Etats du monde se dotent d'un système de protection approprié avant de pouvoir mettre en ligne des données personnelles.

§2. La licéité des transferts en l'absence de décision d'adéquation de la Commission européenne.

En l'absence d'une décision d'adéquation rendue par la Commission européenne et dans le but de ne pas paralyser les opérateurs du secteur du numérique, l'exportation peut être considérée comme licite dans plusieurs cas. En plus des hypothèses légales (A), les responsables de traitement peuvent transférer des données personnelles en dehors de l'Union en ayant recours à des clauses contractuelles types (B), ou à des règles d'entreprise contraignantes (C).

[102] *arrêt CJCE, 6 novembre 2003, n° C-101/01, dit « Lindqvist »*

A. Les exceptions légales à l'illicéité du transfert en l'absence de protection adéquate des données.

Le transfert de données personnelles dans un Etat n'assurant pas un niveau de protection adéquat demeure possible dans certaines hypothèses. L'article 69 de la loi « informatique et libertés » énumère ces cas particuliers. Elle permet ainsi les transferts de données lorsque : la personne concernée a explicitement donné son consentement pour qu'il y soit procédé ; le transfert est nécessaire à l'exécution d'un contrat passé avec la personne concernée ; le transfert est nécessaire à l'exécution d'un contrat passé entre le responsable du traitement et un tiers et ce, dans l'intérêt de la personne concernée. Est également autorisé un transfert nécessaire ou juridiquement obligatoire pour la sauvegarde d'un intérêt de sécurité publique ou dans le cadre judiciaire ; ou bien nécessaire à l'intérêt vital de la personne concernée.

Sous l'influence du Parlement européen, l'article 48 du RGPD empêche un transfert de données effectué sur demande d'un Etat tiers à l'Union européenne en dehors d'un accord international passé avec l'Etat en question. Cette disposition a été influencée par le programme PRISM et vise principalement les pouvoirs de réquisition que se confèrent les autorités gouvernementales américaines dans le cadre du « Patriot Act » et de la lutte antiterroriste. En effet, le gouvernement américain peut accéder à n'importe quelle donnée traitée par une entreprise américaine (même si elle n'est pas établie sur le sol américain) ou qui a des intérêts sur le sol américain. Cet énorme pouvoir de réquisition que se réserve le gouvernement américain présente des risques à la fois pour les libertés fondamentales des citoyens européens, mais aussi pour le secteur privé, dans le cadre de la guerre concurrentielle puisque cela représente un énorme avantage en terme d'intelligence économique.

B. La licéité du transfert opéré sur la base de clauses contractuelles.

Pour aider les opérateurs du numérique et favoriser la circulation des données personnelles hors de l'Union en toute sécurité, la Commission européenne publie des clauses contractuelles types. Ces « modèles » ont vocation à s'appliquer entre deux responsables de traitement (un interne à l'Union et l'autre externe) ou entre un responsable de traitement européen et un sous-traitant non européen. Ces clauses instaurent l'engagement contractuel du destinataire des données qu'il respectera bien les fondamentaux de la directive de 1995. Cependant, la Commission européenne n'a élaboré, à l'heure actuelle, qu'une dizaine de clauses contractuelles types. En

France, les transferts de données personnelles opérés sur la base de clauses contractuelles doivent tout de même être autorisés par la CNIL qui rendra sa décision après avoir examiné les engagements du partenaire du responsable du traitement. Ce dernier doit alors justifier de garanties « suffisantes » sur le fait que les données personnelles seront bien protégées et les droits des personnes concernées respectés. Face au nombre de demandes de transfert sur ces fondements - et partisane d'une simplification des formalités - la CNIL a eu l'occasion de délivrer de nombreuses autorisations sur la base de ces clauses contractuelles sans même les évaluer.[103]

Par ailleurs, le concept même de clause contractuelle type a été introduit il y a un certain temps et sa pertinence peut aujourd'hui être sérieusement remise en question. En effet, ces clauses ont été envisagées alors que les transferts de données personnelles étaient encore majoritairement bilatéraux. Aujourd'hui, les transferts concernent souvent de nombreux sous-traitants, qui ont eux-mêmes recours à plusieurs sous-traitants. Cet instrument présente également des limites certaines face au développement du « Cloud computing » puisque les données ont vocation à se mouvoir sans cesse aux quatre coins du monde. Il devient alors complexe, voire impossible, de suivre les clauses contractuelles conclues initialement sur l'ensemble de la vie des données personnelles transférées. Cela explique le travail du G-29 pour développer le système des règles internes d'entreprises en tant qu'alternative réaliste aux clauses contractuelles types.

C. La licéité du transfert opéré sur la base de « binding corporate rules » ou « règles d'entreprise contraignantes ».

Les règles d'entreprise contraignantes ou « Binding corporate rules » (BCR) ont été créées par un travail conjoint des autorités nationales européennes qui avaient anticipé la logique de l'autorégulation prônée par le règlement du 27 avril 2016 des années avant sa publication. En effet, les BCR sont des règles mises en place de manière interne par le responsable de traitement. Elles ne trouvent pas de fondement dans le texte de la directive de 1995. Après que les CNIL européennes aient développé les BCR « conventionnelles » (1), celles-ci ont été adaptées aux réalités actuelles du traitement de données personnelles. Les BCR « sous-traitants » ont alors fait leur apparition (2).

---

[103] Nathalie Mettalinos, « Données personnelles : vers une responsabilisation des entreprises », Expertises des systèmes d'information, mai 2014, page 174

1) Les BCR « conventionnelles ».

L'entreprise non européenne qui aspire à recevoir des données personnelles doit garantir qu'elle assurera une protection adéquate de ces données. Les BCR démontrent ainsi la politique d'une entreprise en matière de protection des données personnelles, le code de conduite qu'elle applique dans le domaine. Pour permettre le transfert de données, les BCR du responsable de traitement doivent être validées par la CNIL ou par l'une de ses homologues européennes. Les BCR sont très utilisées par les entreprises transnationales qui établissent des filiales sur le territoire de l'Union. Elles permettent à tous les organismes d'un même groupe de pouvoir aisément rapatrier les données collectées vers la maison mère.

Dans la pratique, le système des BCR fonctionne bien mais n'apporte pas une véritable simplification des formalités. Absentes des dispositions de la directive de 1995, les BCR ne constituent pas des autorisations de transfert à proprement parler. Par conséquent, le responsable de traitement y ayant recours n'est pas exonéré de l'autorisation de l'autorité nationale compétente pour pouvoir exporter des données. L'autorité compétente doit alors procéder à un examen allégé des conditions du transfert de données, les dossiers présentés pour ce faire devant comporter de nombreuses informations. On peut alors se demander si les BCR ne pourraient pas faire l'objet d'une autorisation unique de la part de la CNIL, qui procéderait à des contrôles a posteriori quant à la réalité de la protection. Une telle solution paraît plus conforme à la logique du RGPD et permettrait d'alléger la charge de dossiers reçus par la CNIL tout en dispensant les opérateurs du numérique de devoir obtenir une autorisation pour chaque nouveau transfert de données à caractère personnel envisagé.

Reste alors à savoir de quelle manière les autorités nationales européennes s'assureraient de la bonne application des engagements pris par les sous-traitants ou les entreprises qui se trouvent dans un Etat tiers et de quelle façon les sanctionner en cas de violation de leurs engagements. Il est donc nécessaire de pouvoir contrôler ces opérateurs sur le territoire d'Etats extérieurs à l'Union européenne. La CNIL a déjà procédé à des vérifications sur place, à l'étranger.
Cependant, de telles pratiques nécessitent d'être acceptées par les Etats concernés qui pourraient s'opposer à des ingérences de la part d'autorités administratives étrangères. Si la coopération internationale des gouvernements semble nécessaire, la construction internationale d'un cadre protecteur des données personnelles en serait d'autant plus appréciable …

2) Les BCR « sous-traitants ».

Comme nous avons pu le voir, les BCR « classiques » sont limitées aux firmes ou aux groupes multinationaux et n'ont pas vocation à s'appliquer dans l'hypothèse où une pluralité d'intervenants extérieurs à l'Union européenne seraient amenés à prendre part au processus de traitement des données personnelles exportées. Ce qui, dans la pratique, en limite considérablement l'utilité. Face aux avantages économiques que représente le « Cloud computing » et à l'exportation croissante des traitements de données personnelles, les autorités nationales ont alors élargi la portée des BCR en créant les BCR « sous-traitants ».

Ainsi, en dehors du cadre d'un même groupe, un responsable de traitement peut proposer à ses clients une « sphère de sécurité » s'appliquant à ses relations avec d'autres opérateurs. Sphère dans laquelle il pourrait transférer comme bon lui semble et, en principe, en toute sécurité, les données personnelles qu'il a pu recueillir. Enfin, l'instruction de ces règles d'entreprises contraignantes pour sous-traitants doit être assurée par les autorités de contrôle des Etats membres. Celles-ci vont alors évaluer le caractère opposable, contraignant et l'effectivité des règles. Elles s'assurent également de la possibilité pour les victimes d'éventuels manquements aux dispositions contractuelles d'exercer un recours en vue de faire réparer le préjudice qu'elles ont pu subir. Vont donc être audités les procédures et outils stipulés dans les BCR (programmes de formation du personnel, mesures de sécurité mises en œuvre, gestion des plaintes, etc.).[104]

[104] *Fabrice Naftalski, « BCR sous-traitans : une solution pour le Cloud Computing », Expertises des systèmes d'information, avril 2013, pages 135 et 136*

II. La diplomatie dans l'exportation des données personnelles : l'édification d'une adéquation sectorielle.

Si la Commission européenne peut prendre une décision d'adéquation aux vues des dispositions applicables sur le territoire d'un Etat tiers à l'Union, elle peut également le faire au regard d'un secteur d'activité spécifique. Elle peut ainsi prendre une décision d'adéquation sectorielle pour décider qu'un Etat tiers accorde un niveau de protection équivalent à celui de l'UE dans un domaine d'activité en particulier ou sur le fondement d'un mécanisme spécifique. Ce principe d'adéquation sectorielle est maintenu à l'article 45 du règlement du 27 avril 2016.
C'est sur la base d'une telle décision que le mécanisme du « Safe Harbor » a pu voir le jour (§1), avant de disparaître pour enfin être remplacé, après d'âpres négociations intergouvernementales, par le « Privacy Shield » (§2).

§1. L'échec essuyé par le mécanisme « Safe Harbor ».

La recherche d'une adéquation sectorielle a conduit la Commission européenne à mettre en place le mécanisme « Safe Harbor » suite à des négociations avec le gouvernement américain (A). Cependant, ce mécanisme a fini par être invalidé par le juge européen car il est apparu que sa mise en œuvre n'aboutissait pas à une protection suffisante des données personnelles européennes (B).

A. L'émergence du « Safe Harbor » simplifiant les transferts de données en direction des Etats-Unis.

Les Etats-Unis ne sont pas considérés par la Commission européenne comme un Etat assurant une protection adéquate des données. Ils ne figurent donc pas dans la liste des dérogations qu'elle publie. Les transferts de données personnelles devraient donc, en principe, être soumis au « régime de droit commun » des échanges transfrontaliers de données personnelles (recueil du consentement, recours à des BCR ou à des clauses contractuelles types).

Toutefois, des négociations ont été entamées dans le cadre des relations commerciales entretenues entre l'Union européenne et les Etats-Unis. Celles-ci ont abouti, en octobre 2000, à la création du mécanisme dit « Safe Harbor ». Il s'agissait d'une sorte de règlement d'exemption autorisant, sous conditions, les transferts de données personnelles européennes en direction des Etats-Unis. Il était question d'un mécanisme d'adhésion, l'exportation des données ne pouvant être opérée qu'en direction des firmes américaines ayant adhéré aux principes du « Safe Harbor ». Ces dernières étant considérées comme assurant un niveau de protection équivalent à celui octroyé par les entreprises de l'UE, le transfert était censé ne comporter aucun risque majeur pour les libertés fondamentales des personnes concernées. La Commission européenne avait reconnu l'adéquation du niveau de protection offert par le mécanisme « Safe Harbor » par une décision en date du 26 juillet 2000.[105]

Suite à cette décision, les autorités nationales de régulation ont eu l'occasion de faire part de leurs doutes quant à la protection effective assurée aux données personnelles des citoyens européens par le « Safe Harbor ». Le G-29 avait, à l'époque, rendu un avis négatif sur la conformité du contenu de l'accord avec les dispositions de la directive de 1995. D'autre part, comme l'indique Vincent Téchené, « *la CNIL, notamment, estimait que 50 % de sociétés se prétendant Safe Harbor ne l'étaient pas en réalité et que, parmi ces 50 %, au moins la moitié n'était pas en conformité avec ce qu'elles déclaraient. La CNIL et certains de ses homologues européens avaient également attiré l'attention, dans ce contexte, sur les insuffisances du Safe Harbor et sur leur volonté de le renégocier* »[106].

Cependant ces avis sont restés ignorés jusqu'à très récemment. En effet, suite aux sulfureuses révélations d'Edward Snowden sur l'opération de « surveillance » PRISM orchestrée par la NSA, il est devenu clair que les données personnelles transférées en direction d'entreprises basées aux Etats-Unis n'étaient pas protégées de manière suffisante. Cela, que les firmes américaines destinataires des données aient, ou non, pris part au mécanisme du « Safe Harbor ».

[105] *Décision de la Commission européenne n° 2000/520/CE du 26 juillet 2000*

[106] *Vincent Téchené, « L'invalidation du Safe Harbor par la CJUE », La lettre juridique n˚629 du 15 octobre 2015, p. 1*

B. *L'invalidation du « Safe Harbor » par la Cour de justice de l'Union européenne.*

Le sort du Safe Harbor s'est joué à l'occasion d'une affaire portée devant la CJUE par un étudiant autrichien, Maximilian Schrems. Celui-ci a fait valoir son droit d'accès auprès de la société Facebook Ireland qui lui a alors transmis une quantité considérable de données le concernant tandis que beaucoup d'entre elles était censées avoir été supprimées. M. Schrems a alors saisi la juridiction irlandaise, dont la haute juridiction a interrogé la Cour de justice de l'Union. Par un arrêt en date du 6 octobre 2015, la CJUE a invalidé le Safe Harbor[107], considérant qu'il n'assurait pas un niveau suffisant de protection pour les données personnelles des citoyens européens et ne leur ouvrait aucune voie de recours pour faire valoir leurs droits devant les autorités ou juridictions américaines. En effet, la Cour indique que les principes posés par le Safe Harbor sont « *uniquement applicables aux organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union* », mais surtout « *sans qu'il soit exigé que les autorités publiques américaines soient soumises (à leur) respect* ».

Il a donc été reproché au mécanisme un certain manque de transparence quant à l'auto-certification des entreprises et l'absence d'un contrôle suffisant par les autorités nationales. Par ailleurs, ce n'est pas tant la possibilité d'une intrusion du gouvernement américain dans les données personnelles transférées qui pose problème au juge européen - une telle intrusion est légitimée par l'impératif de la sécurité du territoire – que le fait qu'une telle ingérence du droit américain soit généralisée et que rien ne permet aux personnes concernées de s'opposer à d'éventuels abus remettant en cause l'adéquation de protection accordée par le « Safe Harbor ».

Dès lors, les données personnelles ne peuvent plus être transférées aux EU sur la base du « Safe Harbor ». Les Etats-Unis retombent alors dans le régime dérogatoire commun à tous les Etats n'assurant pas une protection adéquate des données personnelles. Les transferts doivent alors être réalisés sur la base du consentement des personnes concernées, des BCR, ou des clauses contractuelles types. Cependant, l'opération PRISM n'ayant pas été stoppée par le gouvernement américain, ces dérogations ne suffisent pas, elles non plus, à assurer un niveau de protection adéquat. La CNIL allemande a ainsi exprimé le souhait d'interdire purement et simplement le transfert de données personnelles européennes en direction des Etats-Unis. Cette

[107] *arrêt CJUE, 6 octobre 2006, n° C-362/14, dit « Schrems »*

situation n'étant pas envisageable, d'un côté comme de l'autre, de nouvelles négociations ont été entamées entre le gouvernement américain et la Commission européenne dans le but d'obtenir une modification de la législation américaine ainsi qu'un nouveau mécanisme dérogatoire pour l'exportation des données. Ces négociations se sont alors tenues autour d'un nouveau mécanisme : celui du « Privacy Shield ».

§2. Le « Privacy Shield » : une meilleure protection pour les données transférées outre-Atlantique ?

Pour remplacer le « Safe Harbor » et remédier à la situation pour le moins inconfortable dans laquelle le vide qu'il a laissé a placé les acteurs du numérique européens, les négociations entre les Etats-Unis et l'Union européenne se sont soldées par un accord. Ainsi, le 12 juillet 2016, la Commission a publié les accords créant le mécanisme du « Privacy Shield ». Le « Privacy Shield » peut s'analyser comme une sorte de « Safe Harbor 2.0 », renforçant les principes et les garanties portés par ce dernier (B). Cependant, certaines disparités juridiques peuvent se faire sentir entre les deux systèmes juridiques en présence. Bien que celles-ci ont tendance à se réduire au fil du temps, comme l'illustre l'appréhension de la notion même de données à caractère personnel (A), les impératifs sous-tendant ces deux systèmes de régulation ne sont pas les mêmes. C'est pourquoi de sérieux doutes subsistent quant à la réalité de la protection conférée par le « Privacy Shield » aux données personnelles européennes (C).

A. Le périmètre du « Privacy Shield » : entre donnée personnelle et « personally identifiable information ».

Tout d'abord, il faut aborder une différence conséquente entre la notion de « données à caractère personnel » et de « Personally indentifiable information » (PII), notion de droit américain. En effet, le terme de PII renvoi nécessairement à des données permettant d'identifier directement un individu.[108]

La conception du caractère « personnel » des données est donc plus restreinte qu'en Europe où, comme nous avons déjà eu l'occasion de le voir, celui-ci peut également renvoyer à une

[108] *Gregory VOSS, « Le concept de données à caractère personnel : divergences transatlantiques Safe Harbor et Privacy Shield », Dalloz IP/IT 2016 p.119*

technique de croisement des données permettant de ré-identifier une personne. Cette différence sensible entre les deux notions déteint sur la capacité des institutions européennes et américaines à négocier dans ce domaine.

Une telle différence pose en effet d'importantes questions dans le contexte du développement du Big Data, où les données sont désidentifiées et n'entrent donc plus dans le périmètre de la notion de PII. Elles échappent ainsi aux dispositions américaines de protection des données personnelles. Or, ceci n'est absolument pas le cas dans l'Union européenne, que les données collectées soient anonymisées ou simplement « pseudonymisées ». Le G-29 considérant d'ailleurs que « *la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile* ».[109].

La notion de donnée personnelle revêt donc toute son importance dans le cadre du « Privacy Shield » puisqu'elle va permettre de fixer le périmètre de la protection des données transférées outre-Atlantique. En effet, si celle-ci n'est pas suffisamment large, elle ne peut pas permettre une protection suffisante et aboutira à l'abolition du « Privacy Shield ». La définition retenue par le « Privacy Shield » penche en faveur de la conception européenne de la notion de donnée personnelle puisque le texte indique que celle-ci doit être entendue comme toute donnée identifiante ou permettant l'identification d'un individu, quelle que soit la forme sous laquelle la donnée se présente. L'appréciation du caractère personnel de la donnée doit se faire à partir du cadre posé par la directive de 1995.

Même si cette conception élargie du périmètre de la protection affichée par le « Privacy Shield » dépasse la conception classique de la PII, des questions peuvent se poser quant à son application aux Etats-Unis. On peut ainsi se demander comment les opérateurs économiques, les autorités administratives et les juridictions américaines vont pouvoir apprécier de manière efficace un concept de droit étranger auquel ils ne sont pas foncièrement familiarisés ?

[109] *G-29, Avis sur les techniques d'anonymisation, 10 avril 2014, p. 3*

B. Les améliorations de la protection apportées par le « Privacy Shield ».

De nombreux principes portés par la législation européenne sont repris dans le « Privacy Shield » dans le but de renforcer la protection des données personnelles des citoyens européens. Ainsi, l'information des individus doit être renforcée quant aux données collectées, à la finalité du traitement envisagé, à l'existence d'un droit d'accès et d'un organe indépendant de résolution des litiges. Les données doivent, là encore, être collectées lorsqu'elles sont nécessaires à la finalité du traitement (principe de proportionnalité).

De plus, certains des reproches faits à l'endroit du « Safe Harbor » ont été pris en compte lors de l'élaboration du « Privacy Shield ». Ainsi, les entreprises américaines devront faire preuve d'une plus grande transparence en publiant les engagements qu'elles prendront. La lutte contre les auto-certifications frauduleuses sera accentuée par les autorités de contrôle américaines, qui auront la possibilité de sanctionner ou d'exclure du mécanisme les acteurs récalcitrants. Ce principe de transparence s'appliquera également à l'administration américaine dans le cadre de la sécurité nationale. Par ailleurs, les autorités américaines se sont engagées à ne plus procéder à des prélèvements massifs de données personnelles pour répondre à cet objectif mais à se restreindre à des collectes ciblées. L'ingérence du gouvernement américain sera alors limitée et des mécanismes de supervision seront mis en place.

D'autre part, les litiges seront résolus par un médiateur (« Ombudsman »), lui-même indépendant des services de renseignement et qui assurera le suivi des plaintes et des demandes d'information des particuliers. Pour finir, le droit de recours des citoyens européens sur le territoire américain est renforcé de manière significative, ce qui résulte de l'adoption du « Judicial Redress Act » par le gouvernement américain le 24 février 2016. En effet, les citoyens européens auront la possibilité d'adresser leurs plaintes à l'autorité nationale compétente d'un des Etats membres de l'Union européenne. Celle-ci transmettra alors la plainte aux autorités nationales américaines. Cette simplification des saisines par les particuliers s'accompagne de la possibilité de passer par un mode alternatif et gratuit de régulation des litiges lorsqu'ils n'auront pas été réglés par la voie « classique ».

Afin de s'assurer du bon fonctionnement du « Privacy Shield » dans la pratique et dans le temps, un mécanisme de réexamen annuel est prévu. En plus du secteur privé, l'examen s'appliquera également à s'assurer du respect des engagements concernant l'accès aux données à des fins

d'ordre public et de sécurité nationale. Il sera opéré de manière conjointe par la Commission européenne et le Ministère du commerce américain qui feront appel à des experts travaillant au sein d'autorités de protection des données personnelles des deux continents.

C. Les limites apparentes présentées par le mécanisme du « Privacy Shield ».

Peu de temps après la publication du « Privacy Shield », le G-29 a rendu un avis faisant étant du point de vue et des doutes émis par les autorités de régulation européennes en ce qui concerne son efficacité.[110] Ainsi, le G29 a commencé par regretter l'absence ou l'insuffisance de plusieurs principes tels que celui de finalité (qui n'est pas fixé clairement par le texte), la limitation de la durée de conservation des données (qui n'y est pas mentionnée de manière expresse) et l'interdiction des décisions automatisées prises sur la base de l'exploitation de données personnelles. Il a ensuite dénoncé le déséquilibre des obligations de transparence imposées aux entreprises américaines par rapport à celles incombant aux entreprises européennes. Ce déséquilibre serait, selon lui, susceptible d'engendrer des distorsions concurrentielles entre les opérateurs des deux continents.

Par ailleurs, les autorités américaines ont donné des assurances formelles que le « bouclier de protection des données » serait appliqué de façon rigoureuse et que les services nationaux de sécurité ne se livreraient à aucune surveillance de masse. L'avis du G-29 laisse apparaître quelques doutes sur la sincérité de la régulation des traitements sur fond de sécurité nationale. En effet, le « Privacy Shield » laisse la possibilité de recourir à un traitement massif de données personnelles lorsque le traitement ciblé est impossible, et ce, d'autant plus que les annexes produites à l'accord contiennent de simples lettres d'engagement de membres de l'administration américaine actuelle, vouées à être remplacées à l'issue des toutes prochaines élections présidentielles. Il s'agit là de simples engagements non contraignants de l'administration américaine qui n'envisage pas de modifier sa législation en matière de sécurité et d'ordre public. De plus, le G-29 a dénoncé le manque d'indépendance du médiateur « Ombudsman », qui, bien que détaché des services de sécurité nationale, reste dépendant du Ministère du commerce. On peut se demander si ce médiateur sera doté d'une réelle autonomie décisionnelle ou même de pouvoirs suffisants pour faire respecter les droits des citoyens européens en cas de désaccord avec l'administration.

[110] *Avis du G-29 n° WP-238 du 13 avril 2016*

Conclusion

A l'origine, le pacte social assurait à l'Etat le pouvoir d'exercer un certain contrôle sur l'individu. En échange, il garantissait à l'individu la maîtrise de sa sphère intime. Aujourd'hui, l'influence de l'outil numérique sur le dévoilement de soi amène à repenser la nature même de la vie privée et la part qui doit lui être laissée dans les sociétés de l'information. Ainsi, comme a pu l'indiquer la Cour européenne des droits de l'homme, à l'occasion de son arrêt « Rotaru » : « *ce que vous faisiez chez vous, montrer des photos, des vidéos, gérer l'agenda (…) se retrouve dans le cloud* ». Le contexte numérique opère un changement de la notion de « zone personnelle ». Certains, comme Vint Cerf - « évangéliste » de Google - évoquent la notion de « publitude », par opposition à celle de solitude qui est induite par le droit au respect de la vie privée. Ils considèrent que la vie privée est une « anomalie » de l'Histoire liée à la société industrielle du XIX^{ème} siècle. Se dirige-t-on vers une nouvelle construction des droits de l'homme et de la démocratie sous l'ère du numérique ? C'est en tout cas la conception qu'adoptent les majors du numérique. Conception visionnaire ou simple conséquence économique ? Dans le contexte de l'économie de la donnée, la question peut se poser …

Quoi qu'il en soit, la vie privée se distingue du secret et est amenée à être pénétrée, au moyen d'outils numériques, par différents prestataires. Demeurent alors deux solutions : se retirer du réseau - et donc d'une bonne partie de la société - ou ouvrir sa sphère personnelle tout en exigeant des responsabilités accrues pour les acteurs du numérique. La protection de la vie privée, droit individualiste par essence, devient alors paradoxalement le fruit d'une négociation collective.

Par ailleurs, les rapports qu'entretiennent les citoyens avec la protection de leurs données personnelles paraît quelque peu schizophrénique : on retrouve d'un côté une forte demande de régulation mais d'un autre, une implication croissante du numérique dans le quotidien (réseaux sociaux, objets connectés, dématérialisation de l'administration, multiplication des données bien-être, phénomène du « Quantified self », etc.). Le grand public est ainsi attiré par la gratuité fictive affichée dans le marché numérique et par l'espoir de voir se répercuter des retombées positives suite à la communication de leurs données personnelles. Il s'agit là du « paradoxe de la vie privée » : les individus sont inquiets face à l'utilisation qui peut être faite de leurs données

mais les volumes de données personnelles créées augmentent de manière exponentielle. L'Etat de droit doit alors garantir aux citoyens de nombreuses libertés, transposées dans le monde du numérique (liberté d'expression, de communication, d'information, vie privée) ; libertés pouvant d'ailleurs s'opposer entre elles.

Des affaires comme SAFARI, PRISM, Apple c/ le FBI ou encore les déboires judiciaires de Facebook face au juge européen ont grandement contribué à la prise de conscience à l'opinion publique. Elles n'aident pas à favoriser un climat de confiance – nécessaire au développement de l'économie numérique - mais, entretiennent, au contraire, la paranoïa et le sentiment de perte de contrôle. Toutefois, elles permettent aux citoyens d'ouvrir les yeux sur certaines des réalités du numérique. Elles alertent également sur la nécessité de prendre des mesures concrètes et efficaces pour sécuriser leurs libertés fondamentales. Une régulation s'impose alors pour que ce qui était considéré hier comme de la science-fiction, des dystopies littéraires ou cinématographiques, ne soit pas amené à prendre forme réelle. On peut notamment citer le roman « 1984 » - et son décrié « Big Brother » - de George Orwell, dont le pays d'origine est ironiquement le plus équipé en réseaux de télésurveillance au monde, avec une caméra pour 14 habitants dans les rues de Londres. De manière plus terre-à-terre, une régulation rigoureuse semble nécessaire pour éviter l'émergence de milliers de « Little Brothers » que pourraient constituer autant d'entreprises assurant la collecte et le traitement de données personnelles.

Le secteur du numérique est impacté par les évolutions constantes des techniques et des sociétés Sa régulation n'en est que plus ardue. En effet, la lourdeur des procédures normatives, notamment, allonge le temps de réaction du législateur aux phénomènes nouveaux. Cela se vérifie, plus encore, en droit européen. Pour cause, la refonte de la législation européenne en matière de protection des données personnelles n'intervient qu'en 2016, alors que le Projet de règlement était annoncé, de manière officielle, depuis 2012. D'une part, les pouvoirs publics sont amenés à moderniser et à consolider le paysage juridique entourant la protection des données personnelles, ce qui a été entrepris d'une manière efficace au niveau européen à travers le contenu du règlement du 27 avril 2016. Le droit européen vient alors garantir un niveau de protection uniformément élevé de la vie privée des citoyens tout en permettant une meilleure intégration des données personnelles dans le « Marché unique numérique ». D'autre part, les institutions européennes recherchent également la diffusion d'une logique de corégulation, qui permet de faire vivre les textes, de les accompagner dans le temps et à travers les évolutions technologiques. Il s'agit donc d'outil d'adaptation de la régulation « classique ».

Celle-ci se trouve alors renforcée par les pratiques des responsables de traitement, pour une meilleure protection des droits des personnes. La corégulation nécessite une approche pluridisciplinaire et constitue un réel défi, mais également une opportunité considérable pour le droit européen des données à caractère personnel.

Aux approches de régulation et d'autorégulation amorcées par le droit européen, se mêle également la diffusion d'une « culture numérique » auprès du le grand public, de manière à ce que soit rétablie la confiance nécessaire au développement du secteur numérique et aux avancées technologiques et sociales qui en découleront. Les institutions européennes lancent alors un mouvement d'éducation au numérique des citoyens européens, invitant les autorités nationales à y participer. Il s'agit également de redonner aux citoyens européens la maîtrise du « dévoilement de soi » et d'assurer une certaine autonomie de la volonté en matière de données personnelles. De cette façon, les consommateurs se retrouveraient en position de négocier avec les responsables de traitement à travers le marché numérique lui-même. Les citoyens seraient alors en capacité de faire pression pour forcer l'intervention du secteur privé dans la protection de leurs données personnelles. Par conséquent, le RGPD affiche une logique de labellisation et promeut la recherche d'une protection des libertés fondamentales des citoyens européens dès la conception d'un nouveau produit ou service. De manière plus significative, le RGPD met en place un mécanisme d' « accountability », laissant aux responsables de traitement la charge de prouver la conformité de leurs pratiques. Il s'agit là de la véritable révolution amorcée par le règlement. La désignation obligatoire d'un délégué à la protection des données aidera les organismes de traitement à se conformer au mieux à ce mécanisme de responsabilisation du numérique. De plus, le renforcement des pouvoir de sanction des autorités nationales contribue à assurer une protection effective des données personnelles des citoyens européens.

Parallèlement, le législateur européen a dû prendre en considération le fort potentiel économique représenté par les données personnelles. Ainsi, à en plus de réaffirmer des principes forts, garantissant la protection des citoyens, il a dû rechercher à les intégrer dans le marché numérique, européen ou international. De ce fait, il a procédé à une harmonisation des régulations opérées par les Etats membres (notamment en créant un mécanisme de coopération et de cohérence entre les autorités nationales) dans le but de favoriser le développement de l'économie de la donnée sur le territoire de l'Union. Il y a également considérablement simplifié les procédures de transferts de données, assurant une meilleure circulation de l'information.

Enfin, des efforts ont été entrepris pour concilier protection efficace des données et mobilité à l'international. De manière pragmatique, les institutions européennes ont alors développé et renforcé les outils permettant l'exportation des données en toute sécurité dans le monde entier. Ainsi, les BCR « sous-traitants », la négociation du nouveau mécanisme du « Privacy Shield » et l'extension considérable de la compétence territoriale du RGPD sont des avancées significatives dans ce domaine.

Cependant, cet encadrement des flux transfrontaliers de données personnelles s'annonce insuffisant compte tenu du développement du « Cloud computing » et des pratiques de certains gouvernements en matière d'intelligence ou de sécurité nationale. La nécessité de la construction d'un cadre protecteur international semble alors indiscutable. Cela permettrait de dégager un consensus avec les acteurs majeurs du numérique, souvent américains. Une telle entreprise ne remettrait pas en cause les négociations entre l'Union européenne et les Etats-Unis mais assurerait un socle minimal de protection et permettrait d'éviter qu'une éventuelle rupture du « Privacy Shield » ne laisse un vide pesant sur les relations commerciales (comme cela a pu être le cas lors de l'invalidation du « Safe Harbour »). Qui plus est, un cadre protecteur permettrait également d'élaborer des mécanismes internationaux de protection de l'Internet et des données personnelles contre les intrusions et attaques des Etats, agences de renseignement, de particuliers ou encore du secteur privé. Par ailleurs, il serait nécessaire de préserver et de sécuriser les standards du web (sécuriser les algorithmes de cryptage pour assurer davantage d'efficacité aux protocoles de sécurité, par exemple). Par voie de conséquence, cela conduirait à écarter le risque d'occurrence d'une crise de confiance mondiale dans l'Internet ou dans le numérique. Mais de telles constructions internationales sont aujourd'hui difficilement concevables tant les intérêts des Etats diffèrent en matière de numérique.

De par le prisme économique, on observe toutefois un échange culturel opéré à l'échelle internationale en termes de protection des données. Ainsi, par exemple l'Union européenne intègre le mécanisme anglo-saxon de l' « accountability », comme le prônait l'ICO (la CNIL britannique). D'un autre côté, de nombreux pays adaptent leurs conceptions de la vie privée et de la protection qu'ils accordent aux données personnelles pour pouvoir entrer en adéquation avec le droit européen. Bien que cette volonté soit, à la base, guidée par de seuls impératifs économiques, elle n'en demeure pas moins bien réelle. On observe par exemple dans des pays du Pacifique - pourtant plus enclins à laisser le marché s'autoréguler sans passer par les lois nationales – un début d'intégration des principes « informatique et libertés » dans leurs droits

nationaux. L'économie de la donnée tend donc à la diffusion de la régulation européenne des traitements de données personnelles et, de manière plus large, vers un rapprochement entre les systèmes juridiques et culturels. Plus que jamais, la mise en place, dans un futur proche, d'un droit international des données personnelles se laisse pressentir …

Bibliographie

Encyclopédie :

- Lamy « Droit du numérique », Wolters Kluwer, édition 2015, paragraphes 544 à 644
- Guide pratique Lamy, Wolters Kluwer, édition 2015, paragraphes 4260 à 4390

Ouvrages généraux et spécialisés :

- Carine BERNAUD, « Open Access et droit d'auteur », Larcier, 2016 ;
- Jérôme LEFORT, Marion Hainez et Marine Chatelet, « Gérer, sécuriser et valoriser les données personnelles des collectivités territoriales », Territorial éditions, 2016 ;
- Agathe LEPAGE et Haritini MASTSOPOULOU, « Droit pénal spécial », Thémis droit, 2015 ;
- Olivier de MAISON ROUGE, « Le droit de l'intelligence économique », Lamy, 2012 ;
- Fabrice MATTATIA, « Traitement des données personnelles », Eyrolles (2ème édition), 2015 ;
- Éric PERES, « Les données numériques : un enjeu d'éducation et de citoyenneté » (avis du Conseil économique, social et environnemental), Journal Officiel de la République française, janvier 2015 ;

Articles doctrinaux :

- Isabelle BEYNEIX, « 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 Novembre 2015, doctrine n° 1260 ;
- Maryline BOIZARD, « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », Communication Commerce électronique n° 3, mars 2016, étude n° 6 ;
- Céline CASTETS-RENARD, « Le Privacy Shield », Dalloz IP/IT 2016, p. 113 ;

- Céline CASTETS-RENARD, « La transposition de la directive PSI 2 et l'ouverture des données publiques », Dalloz IP/IT 2016, p. 6 ;

- Céline CASTETS-RENARD, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », Dalloz IP/IT 2016, p. 115 ;

- Dany COHEN « Ampleur et qualité du consentement donné par clic de souris », Les petites affiches n° 164, août 2014, p. 3 ;

- Laurent CYTERMANN, « La loi Informatique et libertés est-elle dépassée ? », RFDA 2015, p. 99 ;

  Anne DEBET, « La Commission des clauses abusives et la protection des données personnelles sur les réseaux sociaux : une incursion hésitante dans un territoire inconnu », Revue des contrats n°3, septembre 2015, p. 496 ;

- Olivia DUFOUR, « Rapport annuel de la CNIL : 2015, une année choc ! », Les petites affiches n° 75, avril 2016, p. 4 ;

- Isabelle FALQUE-PIERROTIN, « La CNIL face à l'économie de la donnée », AJ Contrats d'affaires - Concurrence 2016 p.175 ;

- Vincent GAUTRAIS , « Différences culturelles en matière de vie privée : point de vue canadien », Dalloz IP/IT 2016 p.128 ;

- Gérard HAAS, « La cybercriminalité à la fois côté obscur et face cachée du Big Data », Dalloz IP/IT 2016, p. 21 ;

- Maximilien LANNA, « Le quantified self : nouveau moteur du Big Data et menace pour la vie privée », Les petites affiches, mai 2016, p. 6 ;

- Maud LÉNA, « Renforcement de la protection des données personnelles », AJ Pénal 2016, p. 52 ;

- Olivier de MAISON ROUGE, « Un nouveau label CNIL gouvernance informatique et libertés », Lexbase Hebdo - éditions affaires n° 409, janvier 2015 ;

- Winston MAXWELL et Sarah TAÏEB, « L'*accountability*, symbole d'une influence américaine sur le règlement européen des données personnelles ? », Dalloz IP/IT 2016 p. 123 ;

- Nathalie METALLINOS, « Données personnelles : la CJUE renforce les règles de protection », Dalloz IP/IT 2016, p. 47 ;

- Nathalie METTALINOS, « Notification des violations de données à la CNIL : tendre le bâton pour se faire battre ? », Dalloz IP/IT 2°16, p. 98 ;

- Florence MEURIS-GUERRERO, « Une clarification du droit au déréférencement », Communication commerce électronique n° 12, décembre 2015 ;

- Christine NOIVILLE, « Big pharma, big data et recherche génétique en santé », Revue des contrats n° 02, mai 2015, p. 352 ;

- Henri OBERDORFF, « L'espace numérique et la protection des données personnelles au regard des droits fondamentaux », Revue de droit public n°1, janvier 2016, p. 41 ;

- Géraldine PÉRONNE « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », Dalloz IP/IT 2016 p. 192 ;

- Romain PERRAY, « Arrêt Schrems : Cour(s) magistral(e) de droit à la protection des données personnelles », Communication Commerce électronique n° 12, Décembre 2015, étude 21 ;

- Sylvie PEYROU « La protection des données à caractère personnel au sein de l'UE : des enjeux économiques et sécuritaires encadrés par le législateur sous le contrôle du juge », Revue du droit public n°1, janvier 2016, p. 55 ;

- Karine RIAHI, « La proposition de règlement européen relatif à la protection des données à caractère personnel : vers un marché numérique unique ? », La semaine juridique - édition générale n° 9-10, Février 2016, p. 273 ;

- Jacky RICHARD, « Le numérique et les données personnelles : quels risques et quelles potentialités ? », Revue de droit public n°1, janvier 2016, p. 87 ;

- Olivia TAMBOU, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », Revue Lamy de Droit de l'Immatériel, avril 2016, p. 51 ;

- Vincent TÉCHENÉ, « Google et le droit à l'oubli », Lexbase hebdo éditions affaires n° 384, juin 2014, p. 1 ;

- Vincent TÉCHENÉ, « Protection des données personnelles : publication du Règlement au JOUE », Lexbase Hebdo édition affaires n°464, mai 2016, p. 1 ;

- Nathalie VANDELLE, « Le contrôleur européen de la protection des données et la protection des données personnelles dans l'administration européenne », Revue de l'Union européenne 2012, p. 44 ;

- Gregory VOSS, « Le concept de données à caractère personnel : divergences transatlantiques Safe Harbor et Privacy Shield », Dalloz IP/IT 2016 p.119 ;

Articles de presse :

- Henri d'AGRAIN, « 5 questions sur le Règlement Européen de Protection des Données Personnelles » : http://www.informatiquenews.fr/5-questions-reglement-europeen-de-protection-donnees-personnelles-47745 ;

- Amira BOUNEDJOUM, « La commercialisation des données personnelles dans la ligne de mire de la CNIL ! » : http://www.lesechos.fr/idees-debats/cercle/cercle-157928-la-commercialisation-des-donnees-personnelles-dans-la-ligne-de-mire-de-la-cnil-2010000.php ;

- Jean-Yves NAU, « Santé et Big Data: l'échec de Google Flu ne doit pas cacher la forêt » : http://www.slate.fr/story/120441/sante-big-data-echec-google-flur ;

- Caroline PIQUET, « Les données personnelles de 112.000 policiers ont fuité sur le web » : http://www.lefigaro.fr/actualite-france/2016/06/27/01016-20160627ARTFIG00154-les-donnees-personnelles-de-112000-policiers-ont-fuite-sur-le-web.php ;

- Marc REES, « La protection des données personnelles, entre Brexit et Privacy Shield » : http://www.nextinpact.com/news/100410-la-protection-donnees-personnelles-entre-brexit-et-privacy-shield.htm ;

- Cécile THIBERT, « Les données personnelles de santé accessibles aux assurances et laboratoires » : http://sante.lefigaro.fr/actualite/2016/05/30/25032-donnees-personnelles-sante-accessibles-assurances-laboratoires ;

Sites internet :

- http://www.cil.cnrs.fr ;
- https://www.cnil.fr ;
- http://www.consilium.europa.eu ;
- https://www.donneespersonnelles.fr ;
- http://europa.eu ;
- http://www.robert-schuman.eu ;
- https://www.secure.edps.europa.eu ;

Autres :

- Avis G-29 sur l'accord Privacy Shield du 13 avril 2016 : https://www.cnil.fr/fr/communique-g29-publication-de-lavis-du-g29-sur-laccord-privacy-shield ;
- Etude de la Commission européenne, « Data protection eurobarometer 2015 » publiée en juin 2015 : http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf ;
- Vidéo. « Faut-il avoir peur de Google » Documentaire (2006), Sylvain BERGÈRE (réal.) et Stéphane OSMONT : https://www.youtube.com/watch?v=_P8mtEbIook ;
- Vidéo. « La face cachée de Google », Reportage « Envoyé spécial » (2015), Sophie ROLAND, Edouard BRITCH, Gary GRABLI, Vincent KELNER et Aymeric GUILLOT : http://www.francetvinfo.fr/replay-magazine/france-2/envoye-special/video-envoye-special-la-face-cachee-de-google_1148465.html ;

Table des matières

REMERCIEMENTS **6**

LISTE DES PRINCIPALES ABREVIATIONS UTILISEES **7**

SOMMAIRE **8**

INTRODUCTION **9**

PARTIE 1 - HARMONISATION DE LA PROTECTION DES DONNEES PERSONNELLES DANS L'UE. **27**

CHAPITRE 1 : LES CONTOURS D'UNE « DECLARATION DES DROITS DE L'HOMME » A L'ERE DU NUMERIQUE. 29

I. La réaffirmation et l'évolution des principes relatifs à la protection de la personne. *31*

§1. La réaffirmation des droits accordés aux individus par la législation « informatique et libertés ». 31

A. Le droit à l'information de la personne concernée : la recherche de transparence dans le traitement des données à caractère personnel. 31

B. Le droits d'accès accompagnant la logique de transparence du traitement de données à caractère personnel. 32

C. Le droit de rectification, de mise-à-jour et d'effacement assurant à l'individu la maîtrise de ses données personnelles. 33

D. Le droit d'opposition : maîtrise ultime donnée à l'individu sur ses données personnelles ? 34

§2. : L'influence du droit européen sur les évolutions des droits de la personne. 36

A. L'intensification de la protection des données personnelles des mineurs. 36

B. L'introduction d'un droit à la portabilité des données personnelles ; 36

C. L'introduction par le juge européen d'un droit au déréférencement sur l'Internet. 37

1) Les problématiques soulevées par le droit au déréférencement 37

2) La mise en œuvre du droit au déréférencement par l'entreprise Google. 39

II. L'extension de la régulation des pratiques du responsable de traitement. *41*

§1. L'évolution des obligations imposées au responsable de traitement. 41

A. Les restrictions propres à la collecte de données personnelles. 41

1) Le principe de loyauté et de licéité de la collecte, ou « principe de transparence ». 42

2) L'obligation de recueillir le consentement de la personne concernée. 42

3) L'interdiction de traitement des données sensibles. 44

4) Le principe de finalité de la collecte. 46

5) Le principe de proportionnalité de la collecte. 47

B. Les restrictions perdurant durant la totalité de la durée de vie des données personnelles. 48

1) Le principe de conservation limitée des données personnelles ou « principe de temporalité ». 48

2) L'obligation d'assurer la sécurité et la confidentialité des données stockées. 49

3) L'obligation de notifier les failles de sécurité, étendue à tous les responsables de traitement. 51

§2. L'extension de la responsabilité dans le cadre du traitement des données personnelles. 53

A. La responsabilité de l'opérateur établi en dehors du territoire européen. 54
B. Vers une responsabilité étendue à tous les participants au processus de traitement de données personnelles ? 56
CHAPITRE 2 : LA COLLABORATION DES INSTITUTIONS DE REGULATION A LA PROTECTION DES DONNEES PERSONNELLES. 58
I. L'intervention de la Commission nationale de l'informatique et des libertés. 59
§1. Les formalités préalables devant être remplies par les responsables de traitement. 60
A. La déclaration normale : procédure « commune » de formalité préalable. 60
B. L'assouplissement des formalités en présence de risques moindre pour les personnes concernées. 61
1) La dispense de déclaration préalable. 61
2) La déclaration simplifiée. 62
3) La mise en place d'une procédure de déclaration unique par la CNIL. 63
C. L'alourdissement des formalités en cas de traitement à risques. 63
1) La demande d'autorisation ou d'avis de la CNIL. 63
2) L'intervention de la CNIL dans le cadre d'un acte réglementaire unique. 64
§2. Les missions de contrôle et de sanction dévolues à la Commission nationale informatique et libertés. 65
A. Les pouvoirs de contrôles dévolus à la CNIL. 65
B. Les pouvoirs de sanctions dévolus à la CNIL. 67
§3. L'insertion d'un mécanisme de cohérence entre les autorités nationales européennes. 69
II. Les autres autorités intervenant dans le processus de régulation. 70
§1. Le délégué à la protection des données : nouvel acteur-clé de la régulation. 70
A. Le Correspondant informatique et libertés : un relai dans la protection des données personnelles. 70
B. Vers un « CIL 2.0 » placé au cœur de la protection des données personnelles. 72
§2. L'actualisation du G-29 : le nouveau Comité européen de la protection des données. 73
§3. Le contrôleur européen de la protection des données. 74
PARTIE 2 – L'INTEGRATION DES DONNEES PERSONNELLES DANS LE MARCHE ECONOMIQUE NUMERIQUE. 76
CHAPITRE 1 : L'ACCROISSEMENT DES DEBOUCHES COMMERCIAUX POUR LES DONNEES PERSONNELLES : L'INTEGRATION DANS LE « MARCHE UNIQUE NUMERIQUE ». 78
I. Promouvoir la circulation des données personnelles en restaurant la confiance des citoyens européens. 81
§1. Eduquer le public à la protection des données personnelles : un nouveau défi pour les institutions européennes. 82
A. L'adoption d'une approche « relationniste » par la CNIL : l'exemple des supports d'enseignement. 82
B. La lutte contre le dysfonctionnement informationnel : l'exemple des conditions générales d'utilisation. 83
C. La création d'un droit de propriété sur les données personnelles : une « fausse bonne idée » ? 85
§2. Le développement de l'identité numérique comme vecteur de confiance pour les citoyens européens. 86
II. Promouvoir la circulation des données personnelles tout en responsabilisant les opérateurs du numérique 89

§1. L'émergence de l' « accountability » : la responsabilisation des opérateurs du numérique et la recherche d'une corégulation. 89
A. La réduction des charges administratives : l'introduction d'un « contrat de confiance » avec les acteurs du numérique....91
B. Les outils mis à la disposition du responsable de traitement pour assurer la preuve de la conformité de ses agissements....92
1) L'obligation de tenir une documentation détaillée sur les traitements. 93
2) L'obligation de procéder à une étude d'impact en présence de traitements « à risque ». 93
§2. L'émergence d'autres outils d'autorégulation comme vecteurs de compétitivité et de différenciation pour les professionnels du numérique....95
A. L'autorégulation par la protection de la vie privée dès la conception. 95
B. L'autorégulation par l'attrait de la certification. 96
CHAPITRE 2 : LA REGULATION DU TRANSFERT DE DONNEES PERSONNELLES EN DEHORS DE L'UNION EUROPEENNE. 99
I. Le « droit commun » de l'exportation des données personnelles : la recherche d'une protection territoriale « adéquate ». 101
§1. La licéité des transferts reconnue par décision d'adéquation de la Commission européenne. 101
§2. La licéité des transferts en l'absence de décision d'adéquation de la Commission européenne. 103
A. Les exceptions légales à l'illicéité du transfert en l'absence de protection adéquate des données. 104
B. La licéité du transfert opéré sur la base de clauses contractuelles. 104
C. La licéité du transfert opéré sur la base de « binding corporate rules » ou « règles d'entreprise contraignantes ». 105
1) Les BCR « conventionnelles ». 106
2) Les BCR « sous-traitants ». 107
II. La diplomatie dans l'exportation des données personnelles : l'édification d'une adéquation sectorielle....108
§1. L'échec essuyé par le mécanisme « Safe Harbor ». 108
A. L'émergence du « Safe Harbor » simplifiant les transferts de données en direction des Etats-Unis. 108
B. L'invalidation du « Safe Harbor » par la Cour de justice de l'Union européenne....110
§2. Le « Privacy Shield » : une meilleure protection pour les données transférées outre-Atlantique ? 111
A. Le périmètre du « Privacy Shield » : entre donnée personnelle et « personally identifiable information ». 111
B. Les améliorations de la protection apportées par le « Privacy Shield ». 113
C. Les limites apparentes présentées par le mécanisme du « Privacy Shield ». 114
CONCLUSION 115
BIBLIOGRAPHIE 120
TABLE DES MATIERES....125