LA PROTECTION DE LA VIE PRIVEE DES LA CONCEPTION OU L'INTEGRATION DE LA *PRIVACY BY DESIGN* COMME MECANISME DU REGIME GENERAL SUR LA PROTECTION DES DONNEES EN DROIT EUROPEEN

Émilie MOUCHARD

Lex Electronica, vol. 18.2 (Automne/Fall 2013)

Sommaire

Introduction

Pour assurer la libre circulation des données en Europe, il convient d'avoir un niveau suffisant de protection des données[1] dans les États membres, et pour ce faire, il est nécessaire de développer des outils opérationnels et leurs mécanismes d'application[2]. La *Privacy by Design* est un de ces mécanismes, elle vise la prise en compte de la vie privée dès la conception. Portée par Ann Cavoukian depuis 1999[3], elle est aujourd'hui reconnue par le droit européen qui en propose l'intégration dans son projet de refonte[4] du droit à la vie privée.

Dans ce projet, comportant une proposition de directive et une proposition de règlement[5], l'Union Européenne marque une volonté générale de prévention des atteintes et une évolution de la protection de la vie privée jusqu'alors articulée en trois générations[6]. Cette volonté est la traduction de la troisième génération dans laquelle nous entrons actuellement, qui pose un besoin de refonte du régime pour aller plus en profondeur dans l'efficience de la protection et éviter toute atteinte.

---

1 Le terme générique de "protection des renseignements personnels" trouve son pendant européen sous le vocable "protection des données personnelles". L'utilisation du terme "donnée personnelle" ne reflète en rien un choix de différenciation entre "renseignement personnel" et "donnée personnelle" mais plutôt une adaptation du terme au contexte du sujet en l'occurrence le droit européen.

2 Alexandra Guerin-Francois « Encadrements juridiques et champs d'application de la Privacy by Design », conférence donnée dans le cadre de l'atelier *Privacy by Design, mettre la technologie au service de la vie privée : enjeux, limites et perspectives*, Paris, le 23 mars 2012, en ligne : http://www.ceric-aix.univ-cezanne.fr/fileadmin/CERIC/Documents/manifestations_scientifiques/Atelier_Privacy_by_design/CNIL-Mme_Guerin_Francois.pdf.

3 Commissaire à l'information et à la protection de la vie privée de l'Ontario, http://www.ipc.on.ca/french/home-page/ (consulté le 14 juin 2013).

4 *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données*, COM(2012) 10 final - *Proposition de règlement du Parlement européen et du Conseil du 25 janvier.2012 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 (règlement général sur la protection des données)*, COM(2012) 11 final .

5 La directive est un texte qui a pour but de fixer des objectifs aux états membres pour que ceux-ci les transposent en accord avec leur législation interne. Le règlement est lui un texte d'application directe, il est obligatoire dans tous ces éléments dès sa publication et est d'application immédiate.

6 YVES POULLET, « *Pour une troisième génération de règlementation de protection des données* », dans *Défis du droit à la protection de la vie privée = Challenges of privacy and data protection law*, Namur, Bruxelles, Crid Facultés universitaires Notre-Dame de la Paix de Namur, Bruylant, 2008, p. 25-70.

Un exemple de ce besoin de refonte des mécanismes de protection s'illustre par l'affaire dite des « *Google Cars* » pour laquelle l'autorité française de protection des données personnelles, la CNIL[7] a prononcé le 17 mars 2011 une sanction pour infraction aux règles relatives à la collecte licite et loyale des données, manquement au respect de la vie privée et des libertés individuelles, et acquisition d'un avantage concurrentiel du fait de ces manquement (notamment en matière de données de localisation) rendu possible par une absence de contrôle a priori du matériel technologique embarqué dans les véhicules[8].

La *Privacy by Design* est un mécanisme de protection qui a pour but de prendre en compte des questions de protection des données personnelles dès la conception des produits. Cependant, il est important d'y appliquer un contrôle. Ce contrôle se matérialisera par l'intervention d'un « délégué à la protection des données », qui sera en charge de veiller à la bonne application de la protection des données personnelles.

I - Un mécanisme issu d'un besoin accru de protection

1.1. Un mécanisme en trois générations

1.1.1 La première génération : Les principes

La première génération de protection des données personnelles est apparue dans les années 1970 et 1980. Elle coïncide avec la prise en compte d'un régime général de protection de l'individu porté par les chartes et la reconnaissance du volet post-moderne de la société.

Le but était d'assurer la reconnaissance d'un droit : le droit de protéger sa vie privée contre toutes atteintes[9]. À cet effet, les États vont mettre en place un cadre juridique général

---

[7] Il s'agit de la Commission nationale informatique et liberté (CNIL) - http://www.cnil.fr (consulté le 14 juin 2013).

[8] Délibération n°2011-035 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc., Paris, France, 17 mars 2011, disponible http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/D2011-035.pdf (consulté le 14 juin 2013).

[9] « *La protection des données à caractère personnel est un droit distinct du droit à la vie privée, bien que ces deux droits soient étroitement liés.*

Le respect de la vie privée a été institué en 1950 avec l'adoption de la Convention européenne des Droits de l'Homme - dans le cadre du Conseil de l'Europe. En substance, le droit à la vie privée peut être décrit comme un droit empêchant les autorités publiques de prendre des mesures qui constituent une ingérence dans la vie privée, à moins que certaines conditions soient réunies.

Lex Electronica, vol. 18.2 (Automne/Fall 2013)

visant à encadrer les pratiques en matière de traitement des renseignements personnels des individus.

Cette génération initiale de protection des données personnelles fait face à un premier obstacle au sein des États où elle a vocation à être appliquée. En effet, la définition donnée à la notion de vie privée n'est pas la même d'un État à l'autre. Or, la définition de cette notion centrale doit être harmonisée du fait du caractère mondial et global du traitement de l'information. De cette collaboration entre les États résultera la mise en place d'un régime général de protection de la vie privée des individus. Il convient donc d'accorder les visions européenne[10] et nord-américaine[11] de la vie privée autour d'un même cadre, d'une même protection.

Cette harmonisation de la protection a donné lieu au texte de l'OCDE de 1981 posant les règles de protection au travers des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*[12].

Cette idée de protection a également donné naissance à la *Convention 108* de l'Union européenne de 1981[13] ou encore *la Loi sur la protection des renseignements personnels* entrée en vigueur en 1983[14].

Le droit à la protection des données a été introduit dans les années 80 à la suite des évolutions technologiques. En substance, les principes relatifs à la protection des données visent à établir les conditions dans lesquelles il est légitime et licite de procéder au traitement de données à caractère personnel. La législation relative à la protection des données oblige les personnes chargées du traitement à respecter un ensemble de règles et confère des droits aux personnes concernées. Enfin, elle prévoit un contrôle par des autorités indépendantes. »
Site internet du contrôleur européen de la protection des données, sur la législation relative à la protection des données, disponible à http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/EDPS/Dataprotection/Legislation (consulté le 3 avril 2013).

[10] « *Droit au respect de la vie privée et familiale : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* » *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E., n°5 (entrée en vigueur le 3 septembre 1953) [Convention européenne des droits de l'homme], art. n°8.

[11] 4e amendement de la Constitution américaine « the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized ».

[12] OCDE, *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel* (Paris, OCDE, 1981).

[13] *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28.I.1981 ; voir aussi *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JO 07 janvier 1978, p. 00227.

Ces textes posent les bases d'un régime général de protection ainsi qu'une définition des termes centraux de la protection tels que les renseignements personnels[15].

Tout ceci ne peut être efficient que si cette protection est assurée par un contrôle de la part des autorités pour permettre la réparation des atteintes. C'est ainsi que se met en place la deuxième génération de protection des données personnelles qui instaure un mécanisme de contrôle externe pour assurer une balance des intérêts.

1.1.2 La deuxième génération : La coercition

Une fois les bases posées, il convient d'assurer leur mise en œuvre. Pour ce faire des institutions de contrôle sont mises en place afin d'en assurer le respect.

Ces institutions représentent un mécanisme spécifique, qui se matérialise par la création d'autorités de protection des données personnelles[16] et la mise en place de textes fondamentaux détaillant les régimes de protection et leur mise en œuvre.

Dans le cadre de cette deuxième génération, on voit apparaître des textes comme la *directive européenne 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* de 1995[17].

---

14 *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21.

15 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28.I.1981, art 2.a « Toute information concernant une personne physique identifiée ou identifiable » ; *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21, art 3 « Les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable ».

16 Pour le Canada, il s'agit du Commissariat à la protection de la vie privée du Canada (CPVP) (*Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21 et *Loi sur la protection des renseignements personnels et les documents électroniques* L.C. 2000, ch. 5) ; pour le Québec, il s'agit de la Commission d'accès à l'information (CAI) (*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.C., ch A-2.1 et *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch P-39.1) ; pour la France il s'agit de la Commission Nationale de l'Informatique et des Libertés (CNIL) (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, JO 07 janvier 1978, p. 00227) ; au niveau européen, le groupe de travail de l'article 29 réunit l'ensemble des responsables des différentes autorités de protection des données (*Règlement (CE) n° 45/2001 du Parlement européen et du conseil 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*, JOCE, L8/1 du 12 janvier 2001).

17 *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* J.O.C.E., L 281, 23/11/1995.

La directive dispose d'un mécanisme général de protection des données personnelles et reprend les définitions sur la notion de renseignement personnel[18] et la notion de traitement de ces renseignements[19].

Il est ajouté à ce régime général un chapitre VI dédié aux « *autorités de contrôle et groupe de protection des personnes à l'égard du traitement des données à caractère personnel* »[20] qui détaille le régime relatif aux autorités de contrôle. Ce régime sera par la suite encadré par le règlement 45/2001[21].

Le pendant québécois de la directive de 1995 est la *Loi sur la protection des renseignements personnels dans le secteur privé*[22] qui pose le régime général de protection. Son contrôle est assuré par la Commission d'accès à l'information[23].

Au niveau fédéral, la *Loi sur la protection des renseignements personnels*[24], ainsi que la *Loi sur la protection des renseignements personnels et les documents électroniques*[25] disposent que la mission de contrôle est assurée par le commissaire à la protection de la vie privée du Canada[26].

---

18 prec. note. 15 .

19 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28.I.1981, art 2.c « traitement automatisé s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion » ; Directive 95/46/CE du Parlement européen et du Conseil, 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, J.O.C.E., L 281, 23/11/1995, art 2.b « traitement de données à caractère personnel (traitement): toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, tels que 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».

20 Directive 95/46/CE du Parlement européen et du Conseil, 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, J.O.C.E., L 281, 23/11/1995, articles 28 - 29 – 30.

21 Prec note 5

22 *Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q 1993, c. P-39.1.*

23 *Id*, article 41.1 .

24 prec. note. 16.

25 *Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.*

26 *Id*, art 11 et suivants ; prec. note. 16, art 29.

La mise en place des autorités de contrôle résultant de ces textes, a pour but d'assurer l'effectivité de la protection, de palier et sanctionner les dérives si les principes posés n'ont pas été respectés.

Ce mécanisme de contrôle *a posteriori* des principes de protection a vu son efficacité remise en cause dès 2008 par des personnalités comme Peter Hustinx[27], Yves Poullet[28], ou encore Colin Bennet et Charles Raab[29]. Ils font valoir l'idée que la protection ne peut être efficiente si elle n'est pas menée en concertation avec les différents acteurs en présence. À ce titre, Yves Poullet mentionne la nécessité d'une troisième génération de protection des données personnelles pour appréhender les questions de vie privée, basée sur l'action *a priori* et la mise en œuvre d'un régime plus prospectif pour assurer ainsi une efficience de la protection à chaque étape du traitement.

1.1.3 - La troisième génération : La prévention

Pour assurer la légitimité de sa démarche Yves Poullet raisonne par analogie avec la législation sur la sécurité routière. Il mentionne ainsi que :

> « Sur le réseau routier, la législation a imposé certaines règles à ses usagers afin, non seulement d'éviter des accidents, mais aussi de régler de manière équitable les droits et obligations réciproques des différents usagers de la route, avec en général, une propension prétorienne à protéger tout naturellement l'usager le plus faible. Pour ce faire, au-delà du code de la route, est apparue la nécessité d'une intervention législative toute particulière afin de règlementer le réseau routier lui-même ainsi que les véhicules qui sont admis à y circuler, moyennant le respect de certaines normes obligatoires »[30]

Le droit relatif aux usagers de la route s'est construit en trois temps. Dans un premier temps, le législateur a mis en place un code recensant les règles générales, les droits et

---

27 Peter HUSTINX, *Privacy by Design : Tenir les promesses, Respect de la vie privée dès la conception (Privacy by Design) : le séminaire définitif*, Madrid, 2 novembre 2009.

28 Prec. note. 6.

29 Colin BENNETT et Charles RAAB, *The Governance of privacy : policy instruments in global perspective*, Burlington, Ashgate, 2003.

30 prec. note. 6, p70.

obligations des usagers en exposant les comportements conformes. Dans un deuxième temps, une règlementation spécifique s'est appliquée au réseau routier pour assurer une efficience de la protection des usagers par la sanction des comportements contraires aux règles de protection. Et enfin, pour assurer une complète efficience de la protection, le législateur a règlementé les véhicules par des normes obligatoires.

Prenons un exemple fictif pour illustrer nos propos. Sur un réseau routier quelconque, la règle est de ne pas rouler à plus de 100 km/h. Pour assurer la protection des usagers, l'État donne aux agents de police le pouvoir de contrôler cette vitesse et de sanctionner lorsqu'ils constatent des atteintes à la règle. Or, certains constructeurs d'automobiles proposent des moteurs puissants qui incitent les usagers à aller au-delà de la limitation de vitesse posée par la loi. En pareilles circonstances, il convient de sensibiliser non seulement les individus à la sanction qu'ils encourent en cas de dépassement de la limitation de vitesse, mais aussi les constructeurs à la réglementation routière. L'État va poser des règles spécifiques, lors de la construction des véhicules, pour empêcher les constructeurs de proposer des véhicules trop puissants dépassant trop facilement les limitations posées par les règles générales de sécurité routière.

Transposée au domaine de la protection des renseignements personnels, la troisième génération de protection des données personnelles règlementerait l'outil technique et ferait peser sur les fournisseurs d'équipements une obligation de respecter les règles de protection des données personnelles dès le stade de la conception de ces équipements. Cette démarche permettrait ainsi d'accroitre la protection en s'assurant du respect des règles de droit dès les premiers stades de conception des équipements, avant même toute atteinte éventuelle.
Ce mécanisme préventif assurerait une complète efficience de la règle de droit et garantirait l'effectivité de la protection tout en réduisant les dérives.

En mettant en œuvre une collaboration accrue des autorités de protection et des entreprises, l'objectif est de mettre en place un régime de responsabilité répondant aux exigences de transparence, d'efficience et de confiance, et au-delà, de développer un nouveau modèle d'entreprise, celui de « l'organisation responsable »[31].

[31] prec. note. 27.

En effet, en intégrant les entreprises au processus, on assure une idée de responsabilité par la flexibilité. Les autorités de protection des données personnelles se verront ainsi attribuer un pouvoir de négociation dans la mise en place du régime général de responsabilité du traitement des données personnelles, mais également, un pouvoir de sanction. L'État délègue donc tous ses attributs aux dites autorités de protection des données personnelles. Les autorités disposeront ainsi d'un pouvoir d'élaboration des normes et d'un pouvoir de coercition quant à l'application de ces normes. Les responsables de traitements, en tant que gestionnaires des données, pourront ainsi faire part des difficultés rencontrées dans la mise en œuvre du processus et suggérer des solutions afin que la législation y remédie.

Le but des autorités de protection des données personnelles est donc de collecter les informations pour ensuite mettre en place le régime juridique adapté, en collaboration avec les responsables de traitement des données personnelles. Ce mécanisme permettra à l'État, au droit et aux technologies utilisées par les entreprises, de s'adapter. Les questions juridiques ainsi soulevées, seront mieux ciblées et résolues. La collaboration dans l'élaboration des règles de protection sera ainsi gage d'efficacité.

Différentes possibilités peuvent être envisagées dans le cadre du développement collaboratif du régime général de responsabilité du traitement des données personnelles. Comme nous l'avons vu, l'idée générale est celle d'une collaboration entre les acteurs et les États. Mais il existe également d'autres alternatives pour assurer l'efficience, la transparence ainsi que la confiance ; tels que l'autorégulation des acteurs, l'élaboration de mécanismes de *soft law* (en ce sens que des règles sont établies sans toutefois avoir de mécanisme de sanctions proprement juridiques), l'obligation de reddition de compte (présente dans le concept d'*accountability*) ; ou encore, et c'est là que se concentrera notre propos, différents mécanismes de régulation par la technique, et plus spécifiquement par le concept de la *Privacy by design*.

1.2 - Un besoin illustré par la jurisprudence : l'affaire des « *Google Cars* »

1.2.1 - Une atteinte à la protection des données

L'affaire la plus à même d'illustrer la nécessité de mettre en place des mécanismes préventifs de protection de la vie privée est sans doute l'affaire dite des « *Google Cars* ».[32]
Dans cette affaire, la CNIL[33] a procédé à la condamnation de la société *Google.Inc* à 100 000€ de sanction pécuniaire pour violation de la *Loi Informatique et Libertés* française[34].

En effet la société *Google.Inc* procédait à l'enregistrement de données techniques et personnelles issues de la collecte d'informations opérée par cette dernière, à l'insu des particuliers concernés. Cette collecte avait été rendue possible par un équipement spécifique contenu dans les véhicules chargés de la prise de photos pour le système *Google Street View* et *Google Maps*.

Suite à des contrôles effectués entre la fin de l'année 2009 et le début de l'année 2010, la CNIL a pu constater que les enregistrements allaient au delà de la finalité du système. *Google.Inc* avait effectivement pu ainsi développer une base de données de géolocalisation des plus complètes, pouvant conduire la société à occuper une position dominante dans le secteur des services de géolocalisation[35].
Suite à ces contrôles, la CNIL a alors mis *Google.Inc* en demeure de cesser toute collecte de données et de fournir copie de l'intégralité des données collectées[36].
L'analyse de la collecte a révélé que de nombreuses données concernaient les particuliers. Il s'agissait entre autre de données de connexion aux sites web, de mots de passe de messagerie, d'adresses courriel, ainsi que d'échanges courriels sensibles faisant état de l'orientation sexuelle ou de la santé des particuliers.
La Commission a condamné la société *Google.Inc* à une amende de 100 000 € pour collecte illégale d'informations de nature privée, mais également pour l'acquisition d'un avantage concurrentiel vis-à-vis des sociétés ne disposant pas des mêmes outils de profilage[37].

---

32 prec, note 8.
33 prec. note 7.
34 *Loi n°78-17 du 13 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés* disponible http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig (consulté le 14 juin 2013).
35 prec, note 8.
36 La condamnation de *Google.Inc* fait état que l'entreprise s'est refusée à transmettre la totalité des informations techniques nécessaires à la détermination de l'atteinte à la vie privée, la Cnil a en effet jugé que les informations transmises étaient suffisantes pour constater l'atteinte, mais insuffisantes à déterminer avec exactitude l'ampleur de l'atteinte à la vie privée des individus. Reflétant ainsi le problème des pouvoirs publics face aux « géants du web » et le manque de transparence.

Au regard des faits de l'espèce, la sanction pécuniaire de 100 000 € peut apparaitre dérisoire relativement à l'avantage concurrentiel ayant résulté de cette collecte d'informations opérée en violation du droit à la protection des renseignements personnels des particuliers et aux droits associés à la collecte loyale de données personnelles. Une société pourrait, après analyse des risques encourus et des avantages pouvant potentiellement être dégagés, faire le choix stratégique de continuer de tels agissements dans le futur, le risque de contrôle et de sanction des autorités étant largement minoré par les profits dégagés.

Cette affaire montre non seulement la nécessité et l'importance des contrôles externes, mais elle révèle aussi un besoin de responsabilisation des acteurs. Cette responsabilisation passe par un contrôle des comportements et de la technologie utilisée, mais également par un renforcement des sanctions. L'utilisation de la technologie comme interface à la disposition du responsable de traitement permettrait une responsabilisation efficace des acteurs.

1.2.2 - Un besoin de refonte

L'affaire dite des « *Google Cars* » fait ressortir le besoin de refonte du système de sanctions, tel qu'il existe actuellement, et ce pour assurer une effectivité de la protection tout au long du traitement des données personnelles. Cette affaire a mis en lumière le besoin d'agir dès la conception pour éviter les dérives, ainsi qu'un besoin d'intensification des contrôles de la part des autorités de protection.

Ce besoin de refonte a fait l'objet d'une réponse de l'Union européenne par le dépôt, en février 2012, d'un projet de directive[38] ainsi qu'un projet de règlement[39] proposant une refonte du système posé par la directive de 1995[40].

---

[37] Avantage multiplié par le fait qu'à la même période, *Google.Inc* procédait au développement de son application *GoogleLatitude*.

[38] *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données*, COM(2012) 10 final.

Ces projets prennent en compte les difficultés de l'évolution du droit à la protection des renseignements personnels et choisissent d'intégrer un mécanisme de contrôle par la technique, la *Privacy by Design*. Ce choix de *protection de la vie privée dès la conception*[41] ou *protection intégrée de la vie privée*[42] tend non seulement à accroître les bénéfices à court terme - la protection des atteintes à la vie privée - mais aussi les bénéfices à long terme - la sécurisation de l'usage des technologies et l'installation d'une confiance pour l'ensemble des utilisateurs – résultant de sa mise en œuvre.

La *Privacy by Design* vise à prévenir les atteintes à la vie privée en assurant un contrôle du respect de la règlementation dès la conception des systèmes de traitement des données à caractère personnel, et au-delà promeut la transparence de ces technologies.

L'affaire des « *Google Cars* » fait apparaitre que les acteurs économiques utilisent des mécanismes obscurs. Sous de faux prétextes de sécurité, ils mettent effectivement en place des mécanismes susceptibles d'accroitre leur position sur le marché et bafouent les règles générales posées par les États. La *Privacy by Design* contribuerait à un changement des règles en privilégiant la « lumière à l'obscurité »[43]. Jouant avec les éléments essentiels pour les entreprises que sont les règles du marché et la confiance du public, la *Privacy by Design* mettrait en avant l'idée que *« si vous n'avez rien à cacher, pourquoi vous y opposer ? »*[44].

---

39 *Proposition de règlement du Parlement européen et du Conseil du 25 janvier.2012 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 (règlement général sur la protection des données)*, COM(2012) 11 final.

40 prec. note. 20.

41 Traduction choisie par les institutions de l'Union Européenne.

42 Traduction choisie par Ann Cavoukian.

43 C'est l'idée du principe de Kerckhoffs en cryptographie, selon lui, « *La sécurité d'un cryptosystème doit résider dans le secret de la clé. Les algorithmes utilisés doivent pouvoir être rendus publics* » ainsi, pour assure une protection efficiente, on va utiliser la lumière, la clé doit demeurer secrète, mais tous les autres paramètres sont réputés publiquement connus. Ce fondement s'oppose à la sécurité par l'obscurité. La sécurité repose ainsi sur une tendance dont l'énoncé porte sur le fait que la publicité, la connaissance du système décourage les attaques. Pour plus de précisions, voir : http://www.securiteinformatique.gouv.fr/autoformations/cryptologie/co/cryptologie_CH01_SCH01_U02.html (consulté le 14 juin 2013).

44 Il s'agit ici de l'intégration du principe « *comply or explain* » issu du droit des sociétés.

II. Le concept de Privacy by Design

2.1 - Les origines de la notion

La *Privacy by Design* trouve son origine dans les années 1990 et la doctrine de la commissaire à l'information et à la protection de la vie privée de l'Ontario, Ann Cavoukian. Cette dernière part du principe que pour résoudre efficacement les questions relatives au droit de la vie privée et des données personnelles, il faut traiter le problème à sa source, soit dès la création des informations à caractère personnel.

Durant ses deux premiers mandats, la commissaire a porté son projet et a développé avec son équipe une feuille de route, détaillant la manière dont la *Privacy by Design* devrait être gérée de façon à être pleinement efficiente.

C'est en 2010, lors de la *32e conférence internationale des commissaires à la protection des données et de la vie privée* que son concept a été entériné dans une résolution[45]. Cette dernière encourageait les commissaires à promouvoir les principes de la *Privacy by Design* en tant que principes de base dans le fonctionnement des organisations.

L'Union européenne, dans ses propositions de directive[46] et de règlement[47], a fait le choix d'intégrer la notion de *Privacy by Design* en tant qu'outil complémentaire dans l'élaboration du cadre juridique concernant la protection des données.

---

45 COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (FRANCE), «Projet de résolution appelant à la convocation d'une conférence intergouvernementale aux fins d'adopter un instrument international contraignant sur le respect de la vie privée et la protection des données personnelles», dans 32e Conférence mondiale des commissaires à la protection des données et de la vie privée, 27 - 29 octobre 2010, Jérusalem, (disponible à <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/2010-conf_itlee_resolution_projet_FR.pdf>).

46 *Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données*, COM(2012) 10 final.

47 *Proposition de règlement du Parlement européen et du Conseil du 25 janvier.2012 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 (règlement général sur la protection des données)*, COM(2012) 11 final.

Ainsi, l'article 19 de la proposition de directive[48] de même que l'article 23 de la proposition de règlement[49] prévoient la « *protection des données dès la conception et* [la] *protection des données par défaut* » :

> « La protection des droits et libertés des personnes concernées à l'égard du traitement des données à caractère personnel nécessite de prendre les mesures techniques et organisationnelles appropriées, tant au moment de la conception que de l'exécution du traitement, de sorte que les exigences du présent règlement soient respectées. Afin d'assurer et de démontrer la conformité de ses activités au présent règlement, le responsable du traitement devrait adopter des règles internes et appliquer des mesures adaptées, qui répondent en particulier aux principes de la protection des données dès la conception et de la protection des données par défaut. »[50]

Le responsable de traitement des données[51] sera alors chargé de vérifier la bonne application des règles relatives à la vie privée dès la conception des produits, mais aussi durant toute la durée du traitement des informations à caractère personnel.

---

48 « *Les États membres prévoient que, compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux dispositions adoptées conformément à la présente directive et garantisse la protection des droits de la personne concernée.*
Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules les données à caractère personnel nécessaires aux finalités du traitement seront traitées. ».

49 « *Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée.*

Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques.

La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser d'éventuels critères et exigences supplémentaires applicables aux mesures appropriées et aux mécanismes visés aux paragraphes 1 et 2, en ce qui concerne notamment les exigences en matière de protection des données dès la conception applicables à l'ensemble des secteurs, produits et services.

La Commission peut définir des normes techniques pour les exigences fixées aux paragraphes 1 et 2. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2. ».

50 préc., note 4.

51 prec. note. 48.

2.2 - La définition de la notion

L'idée de la *Privacy by Design* est de mettre la technologie au service de la vie privée[52]. Elle a pour cadre juridique la question du principe de responsabilité des entreprises et plus précisément la question des pouvoirs accordés aux responsables de traitement des données dans ces entreprises.

Le responsable de traitement des données est la personne en charge de l'ensemble de la gestion des données personnelles au sein de l'entreprise. Il s'agit de la personne ressource, celle qui s'assure que l'ensemble des procédures ait été respecté, de sorte que l'entreprise ne contrevienne à aucune norme législative relative à la vie privée.

La traduction la plus souvent utilisée pour la terminologie « *Privacy by Design* » est celle de *respect de la vie privée dès la conception* ou encore celle de *protection intégrée de la vie privée* (PIVP). Dans les deux cas, le but de la *Privacy by Design* est d'intégrer les questions de vie privée dès la conception des produits, protocoles et traitements de données. Au même titre que les directives techniques et marketing auxquelles un concepteur peut se référer dans le cahier de commande d'un produit, il disposerait d'un guide juridique indiquant les normes à respecter dès l'étape de conception du produit. Ce dernier ayant été de la sorte certifié ou labellisé dès sa conception – après qu'une déclaration (*self-certification* ou certification par un *trusted third party*) de conformité aux normes juridiques en vigueur ait été faite – le produit ne pourra plus être remis en cause par la suite.

Ce mécanisme permet de prendre en compte les questions liées au respect de la vie privée et des données personnelles dès les premiers stades de l'élaboration du produit. On aspire ainsi à une compréhension des conséquences avant même toute prise de décision et les impacts qui pourraient en découler.

Lorsqu'elle a procédé à l'élaboration du concept, Ann Cavoukian a mis en exergue le fait que la *Privacy by Design* se développe autour de principes fondateurs. Ces sept principes conduisent à

[52] prec. note 3.

la conception de produits répondant aux normes juridiques relatives au respect de la vie privée. Ce guide se déroule comme suit.

Le premier principe est énoncé comme « *Proactive not Reactive ; Preventive not Remedial* »[53]. On place dès le départ la volonté de mettre en place une approche prospective. On choisit en quelque sorte d'appliquer le proverbe « mieux vaut prévenir que guérir ». L'idée générale est la mise en place de mécanismes qui assurent une protection effective de la vie privée, et ce sans attendre qu'une atteinte soit constatée. C'est en soit un régime juridique qui instaure des mesures de protection des données personnelles proactives et non réactives et préventives plutôt que correctives. Le législateur est ainsi un acteur parmi les autres, devant être en accord avec l'évolution des produits et au fait des atteintes possibles afin de donner l'impulsion nécessaire à la réglementation allant au delà de la seule correction des atteintes.

Le second principe est celui de la « *Privacy as the Default Setting* »[54] ou l'idée d'assurer une protection implicite de la vie privée. C'est l'idée d'intégrer, dans le cadre juridique du droit des données personnelles, le droit à la vie privée en tant que droit fondamental et de ce fait mettre en place des mesures de protection de la vie privée les plus étendues quitte à ce que les individus choisissent de diminuer eux même cette protection[55].

Le troisième est celui de la « *Privacy embedded into design* »[56]. C'est l'idée d'intégrer la protection de la vie privée dès la phase de conception du design du projet – de façon intégrale au corps du projet – de sorte que l'intégration des questions relatives à la vie privée devienne des mesures naturelles pour le concepteur. Juridique et technique seront alors fortement assimilés dans cette phase du projet.

---

53 ANN CAVOUKIAN, «Privacy by Design, The 7 Foundational Principles», (2011) http://privacybydesign.ca/about/principles (consulté le 14 juin 2013)

54 *Id.*

55 COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (FRANCE), préc., note 45 p2.

56 A. CAVOUKIAN, préc., note 53.

Le quatrième principe porte sur le « *positive-sum, not zero-sum* »[57]. C'est l'idée d'assurer une efficience intégrale selon ce que la commissaire à la vie privée de l'Ontario qualifie de paradigme à somme positive. C'est plus simplement l'idée d'une mise en commun des connaissances (techniques et juridiques) autour d'un rapport gagnant-gagnant. Ainsi, la mise en commun des connaissances des juristes et des ingénieurs-concepteurs permettra la création d'un objet « certifié » dès sa sortie, palliant de la sorte les éventuelles modifications ou retraits du marché pour non-conformité du produit aux règles de respect de la vie privée.

Le cinquième fondement de la *Privacy by Design* est le « *end-to-end Security* »[58]. C'est l'idée d'assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements. Ainsi, l'information doit être protégée durant tout son cycle de vie.

Le sixième principe assure la visibilité et la transparence des mécanismes : c'est l'idée du « *keep it open* »[59]. La *Privacy by Design* a ainsi pour but de mettre en œuvre des mécanismes de gestion des données personnelles ouverts c'est-à-dire susceptibles de contrôle par l'utilisateur ou toute personne concernée afin de faire passer la confiance par la transparence. La commissaire à la vie privée pose ainsi une alternative aux pratiques souvent peu connues des entreprises liées à l'internet en prônant le raisonnement que s'il n'y a rien à cacher il ne sert à rien de fermer l'accès.[60]

Enfin, le septième et dernier principe prône l'idée « *keep it user-centric* »[61]. Ce principe général place l'utilisateur et le respect de la vie privée de ces derniers au cœur du raisonnement et comme prémisse de réflexion avant toute action de la part des acteurs. Le droit des données personnelles se doit d'être centré sur l'utilisateur qui, en servant de « produit », aliène une part de sa propre personnalité.

---

57 *Id.*

58 *Id.*

59 *Id.*

60 il s'agit ici de lutter contre les mécanismes de la sécurité par l'obscurité souvent préférée par les organisations pour se protéger.

61 A. CAVOUKIAN, préc., note 53.

Ces différents principes, dans une vision globale, forment les différents rouages de la protection vue par Ann Cavoukian.

III. L'articulation du concept

Comme l'a mentionné Yves Poullet, la mise en perspective de la règlementation des nouvelles technologies doit se faire par la prise en compte et l'intégration de la troisième génération de protection des données personnelles. Il convient ainsi de mettre en place de nouveaux mécanismes de règlementation. La *Privacy by Design* faisant partie intégrante de cette troisième génération, elle doit être prise en considération dans la mise en place du nouveau cadre juridique de protection des données personnelles. Cette dernière n'est toutefois pas suffisante en elle-même et doit s'intégrer dans un processus global, général et harmonisé de protection des données personnelles.

Le concept de *Privacy by Design* est un mécanisme de prévention des infractions au régime général de protection des données personnelles, à ce titre, il intègre pleinement ce régime et en est le premier maillon. S'il est essentiel d'assurer l'intégration du concept dans le régime, il convient de garder à l'esprit que ce concept est gage d'efficacité si, et seulement si, il est associé à des mécanismes de protection plus englobants. La *Privacy by Design* a donc ses limites. Elle porte en son sein un projet de responsabilisation de tous les acteurs devant être associé à des mécanismes de soutien et de contrôle.[62]

3.1 - L'exemple européen

Dans la refonte du cadre juridique 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, l'Union européenne fait le choix d'assurer la protection de ses ressortissants par la transparence en passant par la reconnaissance de la *Privacy by Design*.

62 prec. note. 2.

Cette reconnaissance est présente dans l'article 19 de la proposition de directive[63], ainsi que dans l'article 23 de la proposition de règlement[64] qui prévoient tous deux la « *protection des données dès la conception et* [la] *protection des données par défaut* ».

Le cadre de l'article 19 de la proposition de directive pose le principe de la protection des données dès la conception, il s'agit là d'une obligation générale des responsables de traitement des données personnelles et des sous-traitants. Ainsi, le paragraphe 38 du préambule de la proposition énonce le principe tel que suit :

> « La protection des droits et libertés des personnes concernées à l'égard du traitement des données à caractère personnel les concernant exige l'adoption de mesures techniques et organisationnelles appropriées, afin de satisfaire aux exigences prévues par la présente directive. Afin de garantir la conformité du traitement avec les dispositions adoptées en application de la présente directive, le responsable du traitement devrait adopter des règles internes et mettre en œuvre les mesures appropriées, respectant notamment les principes de protection des données dès la conception et de protection des données par défaut. »[65]

---

63 « *Les États membres prévoient que, compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux dispositions adoptées conformément à la présente directive et garantisse la protection des droits de la personne concernée.*
Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules les données à caractère personnel nécessaires aux finalités du traitement seront traitées. »

64 « *Compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, le responsable du traitement applique, tant lors de la définition des moyens de traitement que lors du traitement proprement dit, les mesures et procédures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux prescriptions du présent règlement et garantisse la protection des droits de la personne concernée.*

Le responsable du traitement met en œuvre des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques.

La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser d'éventuels critères et exigences supplémentaires applicables aux mesures appropriées et aux mécanismes visés aux paragraphes 1 et 2, en ce qui concerne notamment les exigences en matière de protection des données dès la conception applicables à l'ensemble des secteurs, produits et services.

La Commission peut définir des normes techniques pour les exigences fixées aux paragraphes 1 et 2. Les actes d'exécution correspondants sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2. ».

65 préc., note 4 p.23.

Chaque responsable de traitement se voit également reconnaître une obligation de désigner un « délégué à la protection des données » associé à toutes les questions relatives à la protection des données personnelles et disposant des moyens nécessaires à l'exercice de sa mission de contrôle, le tout dans un cadre d'indépendance par rapport au responsable de traitement. Il ne peut ainsi recevoir « aucune instruction en ce qui concerne l'exercice de sa fonction »[66]. Le délégué à la protection des données aura donc pour mission de :

> « Contrôler la mise en œuvre et l'application des dispositions adoptées conformément à la présente directive, notamment en ce qui concerne les exigences relatives à la protection des données dès la conception, à la protection des données par défaut et à la sécurité des données, ainsi que l'information des personnes concernées et l'examen des demandes présentées dans l'exercice de leurs droits au titre des dispositions adoptées conformément à la présente directive »[67]

Dans le cadre de l'article 23 de la proposition de règlement, il est précisé que la Commission dispose du pouvoir d'adopter des actes délégués, et ce, pour une durée indéterminée, s'il lui apparaît nécessaire d'apporter des précisions sur d'éventuels critères et exigences supplémentaires d'exercice de la *Privacy by Design*, pour l'ensemble des secteurs, produits et services. Elle dispose également du pouvoir de définition de normes techniques en passant par la procédure d'examen par un comité.

Ainsi, l'Union européenne par ces projets fait le choix d'un régime juridique général, global, prenant en compte l'ensemble des évolutions de la notion de vie privée et des questions posées par la communauté internationale. Il apparaît alors une nouvelle question qui est de savoir si l'intégration des notions portées peut se réaliser de façon efficace auprès des utilisateurs, des entreprises et des institutions ; de voir si la mise en place de nouvelles fonctions comme le délégué à la protection des données personnelles permettra de lutter contre l'obscurité utilisée par les géants du secteur ; de voir si ce délégué permettra de mettre en place la visibilité et la transparence, et par là même la confiance demandée par les utilisateurs et prônée par la *Privacy by Design*.

---

66 *Id*. section 3, p.44-45.

67 *id*. , article 32 (c), p.45.

L'Union européenne a fait le choix de ne pas tout miser sur la *Privacy by Design,* car dans le cadre d'un régime général ce concept n'apparaissait pas suffisant du fait du spectre limité de la conception.

Le concept de *Privacy by Design* est difficile à mettre en œuvre, car il est à mi-chemin entre deux métiers ou disciplines qui n'ont pas pour habitude de collaborer : les ingénieurs, concepteurs de produits d'une part et les juristes d'autre part. Il convient donc de se demander quel profil de formation sera demandé au délégué à la protection des données, chargé de contrôler l'effectivité de la *Privacy by Design*.

3.2 - La question du délégué à la protection des données

Lorsqu'elle évoque la *Privacy by Design*, la directive fait apparaître un nouvel acteur, le délégué à la protection des données. Déjà évoqué dans la directive de 1995 sous le titre de « détaché à la protection des données à caractère personnel »[68], le projet de directive évoque en effet que celui-ci aura pour mission de :

> « contrôler la mise en œuvre et l'application des dispositions adoptées conformément à la présente directive, notamment en ce qui concerne les exigences relatives à la protection des données dès la conception, à la protection des données par défaut et à la sécurité des données, ainsi que l'information des personnes concernées et l'examen des demandes présentées dans l'exercice de leurs droits au titre des dispositions adoptées conformément à la présente directive »[69]

Comme le mentionne l'article 31 du projet de directive, le délégué à la protection des données est une personne rattachée à l'entreprise, mais doit en être indépendante :

> « Le responsable du traitement ou le sous-traitant veille à ce que le délégué à la protection des données soit doté des moyens d'accomplir les missions et obligations visées à l'article

[68] prec. note. 20, article 18, paragraphe 2.

[69] préc., note 4, art 32 (c) .

32 de manière effective et en toute indépendance, et ne reçoive aucune instruction en ce qui concerne l'exercice de sa fonction »[70]

Le délégué à la protection des données est un mécanisme déjà existant dans le droit européen, mais la directive de 95/46/CE [71], de même que le règlement 45/2001[72] réservaient son action aux institutions européennes, et le mettait en collaboration avec le contrôleur européen à la protection des données.

Le projet de directive a pour but d'étendre son champ d'action aux entreprises. La première version du texte posait comme condition la présence d'une personne publique ou privée et la qualification de « grande entreprise » (c'est-à-dire plus de 250 employés). Cependant, le rapport Albrecht[73] propose d'amender ce projet en basant la mission du délégué à la protection des données sur l'importance du traitement des données personnelles davantage que sur la taille de l'entreprise.

Ainsi, selon l'amendement proposé[74], trois types d'entreprises seraient visées par le contrôle : les « grandes entreprises » ; les entreprises dont les activités de base impliquent des opérations de traitement exigeant un suivi régulier et systématique ; et enfin celles requérant le traitement de données personnelles concernant plus de 500 personnes par an. Il sera alors nécessaire pour le responsable de traitement de se faire « aider » par le délégué à la protection des données personnelles.

L'amendement mentionne également une consultation « préalablement à la conception (…) afin de garantir le respect des principes de protection de la vie privée dès la conception et par défaut ». Selon le modèle allemand, qui a servi de base à la proposition européenne, le délégué à la protection des données serait alors une sorte de vérificateur[75] dédié à la vie privée et

---

70 *Id.* , art 31 al 2.

71 prec. note. 20.

72 Règlement (CE) n° 45/2001 du Parlement européen et du conseil 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 , JOCE, L8/1 du 12 janvier 2001.

73 PARLEMENT EUROPÉEN, Commission des libertés civiles, de la justice et des affaires intérieures, 17/12/2012, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387fr.pdf (consulté le 14 juin 2013).

74 *Id*, amendement 48, p.42.

75 Comme celui présenté aux articles 231 et suivants de la Loi sur les sociétés par actions du Québec.

chargé d'un audit permanent de la société, devant être associé à toutes les décisions sans toutefois être lié aux agissements de la société. Il ne peut être solidaire de la société et doit faire état de tous les agissements qu'il estime ne pas être conforme à la législation en vigueur sur la vie privée.

Le délégué aurait ainsi pour rôle de labelliser chacun des « produits » comme étant respectueux des règles relatives à la vie privée. Il endosserait, par sa signature attestant d'une telle conformité, la responsabilité professionnelle de la protection des données. Le cas échéant, s'il refusait de cautionner certains agissements, certaines pratiques qu'il estime ne pas être en conformité avec la législation, il aurait le devoir d'en référer aux autorités compétentes.

Le délégué permettrait ainsi aux autorités de protection des données de disposer d'un régulateur pour chaque structure, de façon à mettre en place un contrôle et une régulation plus efficace sur la question des données personnelles. Au même titre qu'un vérificateur certifie les comptes d'une société comme étant conforme aux règles comptables en vigueur, le délégué certifierait le produit ou la politique comme étant conforme aux règles relatives à la vie privée et à la protection des données personnelles.

Le délégué à la protection des données disposerait alors d'un rôle transversal. Il apparaît comme une personne ressource, faisant « office de point de contact pour l'autorité de contrôle sur les questions liées au traitement, et consulte celle-ci, le cas échéant de sa propre initiative »[76] ; comme un mécanisme complémentaire de régulation de l'internet.

Cependant, il devient essentiel de préciser la nature des compétences qu'il doit détenir, car un simple juriste ne peut en aucun cas faire état de problème quant à la conception d'un produit s'il ne dispose pas de compétences techniques et pratiques dans le domaine du droit des technologies de l'information.

Le délégué à la protection des données s'inscrit dans la ligne directrice de la redéfinition de politique de protection des données personnelles, tendant à mettre en place ce que Peter Hustinx appelle « l'organisation responsable » :

---

[76] *Id*. article 32 (h).

« il est important d'introduire le principe de « l'obligation de rendre compte » (…) cela signifierait qu'une organisation responsable devrait être capable de démontrer le respect de ses obligations de protection des données. Cette mesure stimulerait l'utilisation des « évaluations des facteurs relatifs à la vie privée » et des « audits sur la gestion de l'information à caractère personnel », et déplacerait l'équilibre en matière de respect de la vie privée ».[77]

Conclusion

Le législateur européen se place dans la troisième génération de réglementation de la protection des données posée par Yves Poullet, il établit un régime général en organisant une refonte des textes pour prendre en compte de risques nouveaux.

Cependant, ce régime général pose la limite de la *Privacy by Design* en ce sens qu'il voit le concept comme un des instruments permettant la mise en place d'un régime global. La *Privacy*

[77] PETER HUSTINX, *Privacy by Design : Tenir les promesses*, Respect de la vie privée dès la conception (Privacy by Design) : le séminaire définitif, Madrid, 2 novembre 2009 , *id*. p2.

by Design ne peut à elle seule assurer un mécanisme efficace pour lutter contre les atteintes à la vie privée, elle doit nécessairement se présenter comme un élément du régime général. La *Privacy by Design* a toute son importance, car elle est à considérer comme le point d'entrée de la transparence dans le régime général de la protection des données personnelles. Cependant, elle n'est pas suffisante, et il convient de renforcer les mécanismes de contrôle *a posteriori*.

La *Privacy by Design* est un mécanisme de règlementation par la technique : elle ne fait pas abstraction des principes fondamentaux liés au droit à la vie privée, elle les intègre, comme le mentionne Yves Poullet :

> « Ce n'est pourtant qu'en appliquant les principes classiques de la protection des données à la technologie, ce troisième larron qui s'invite de manière implicite, mais certaine dans toute télécommunication, que l'informatisation de la société pourra conduire à une société de l'information démocratique, moteur de progrès partout et pour tous »[78]

La *Privacy by Design* est donc une méthode pour faire respecter les principes généraux « classiques » liés au droit à la vie privée et au droit des données personnelles[79]. Si ces principes sont correctement appliqués, la technologie pourra ainsi apparaitre comme une interface entre le responsable de traitement (donc l'entreprise) et l'individu, sujet de la protection. Cette protection sera garantie par des contrôles externes exercés par les institutions étatiques et par les délègues à la protection des données.

Il ne reste plus maintenant qu'à suivre et analyser comment les contrôles des délégués à la protection des données vont être effectués, quels seront leurs moyens d'actions effectifs et leurs résultats, pour, au-delà, voir si leur mission permet la mise en place de l'objectif général qu'est celui de la responsabilisation des acteurs du secteur privé.

---

78 *Id.* p 70.

79 Pour certains, le droit européen utilise le concept de Privacy by Design, en allant au-delà du concept d'Ann Cavoukian en ce sens qu'il fait le choix d'utiliser le concept tout en gardant les concepts déjà existants, il s'agirait du concept de Privacy by ReDesign évoqué par Christian Pardieu.