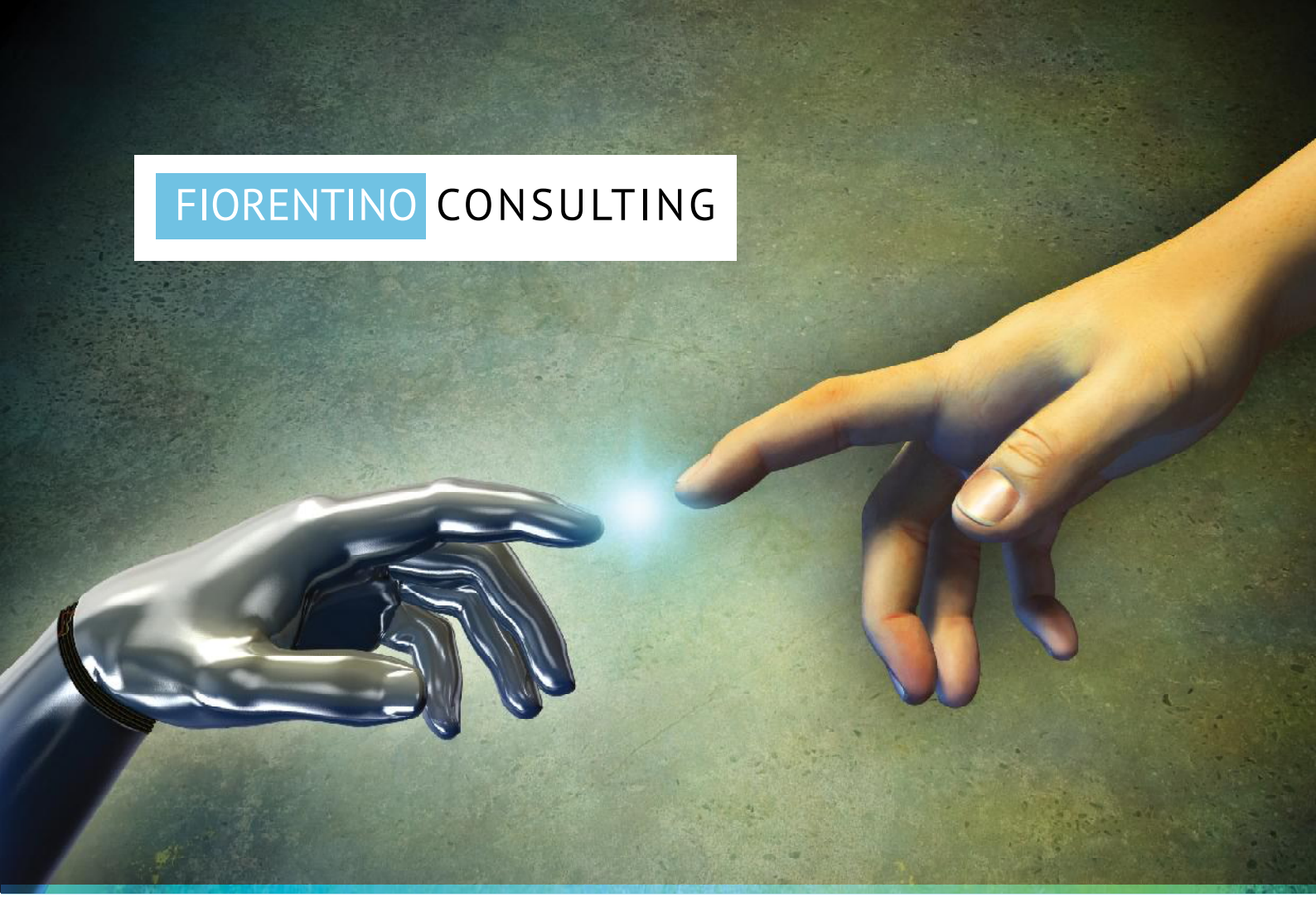
FIORENTINO CONSULTING



PRIVACY BY DESIGN

A LA LUMIERE DU REGLEMENT EUROPEEN

Institut Supérieur d'Electronique de Paris

Mastère Spécialisé en Management et Protection des Données à caractère personnel

Promotion Eric Arthur Blair

Thèse professionnelle soutenue par Alessandro FIORENTINO le 2 décembre 2013

Sous la direction de Claire LEVALLOIS-BARTH
Maître de conférences en droit à l'institut Mines TELECOM/PARITECH
Coordinatrice de la Chaire Valeurs et politiques des informations personnelles

REMERCIEMENTS

Pour commencer nous souhaitons remercier **Madame Claire LEVALLOIS-BARTH,** Maître de conférences en droit à l'institut Mines TELECOM/PARISTECH et Coordinatrice de la Chaire Valeurs et politiques des informations personnelles pour le soutien qu'elle porte à notre démarche.

Nous adressons nos sincères remerciements à **Madame Ann CAVOUKIAN, Ph.D.** Commissaire à l'information et à la protection de la vie privée de l'Ontario au Canada, pour sa disponibilité, son soutien, le temps qu'elle a consacré pour répondre à nos questions et pour l'honneur qu'elle nous a fait en nous invitant à intégrer le programme des ambassadeurs du Privacy by Design.

Nous tenons également à remercier **Madame Karen HALE**, Agent des communications bilingues du Bureau du Commissaire à l'information et à la protection de la vie privée de l'Ontario pour son accueil et son investissement à travers nos différents échanges.

Sans oublier **Monsieur Arnaud VACHER**, Gérant de l'entreprise IRYSIUS pour son soutien et son engagement dans la mise en place de notre programme de formation Privacy by Design au sein de son centre de formation et **Madame Sophie MERINERO**, Correspondante Informatique et Libertés d'IRYSIUS pour avoir initié ce partenariat.

RÉSUMÉ

La commission européenne a publié le 25 janvier 2012 une proposition de règlement général sur la protection des données, ce projet de règlement a pour objectif le renforcement des droits des citoyens et la modernisation du cadre juridique existant permettant à l'Europe de faire face à l'essor du numérique et à la mondialisation.

L'article 23 du projet de règlement intègre la prise en compte de la protection des données dès la conception ainsi que la protection des données par défaut reprenant certains aspects du concept de Privacy by Design reconnu à l'échelle internationale depuis 2010 comme une nouvelle norme mondiale.

La problématique principale de cette thèse professionnelle repose sur le fait de savoir dans quelles mesures ces principes pourront être respectés et mis en œuvre de façon optimale afin que tout organisme qu'il soit privé ou public puisse répondre aux nouvelles exigences introduites afin d'être en conformité avec le nouveau cadre juridique européen.

SUMMARY

The European Commission published on January 25th, 2012 a proposal of general regulation on the data protection. The objective of the project of regulation is to strengthen the rights of the citizens and the modernization of the existing legal framework, allowing Europe to face the development of the digital technology and the globalization.

The article 23 of the project of regulation integrates the consideration of the data protection from the privacy by design as well as the data protection by default, taking back certain aspects of the concept of recognized privacy by design on an international scale since 2010 as a new world standard.

The main issue of this professional thesis is to know in what extend these principles can be respected and implemented in a optimal way so that any body, ruled by civil or public law can answer the new requirements introduced and to be compliant with the new European legal framework.

TABLE DES MATIERES

INTRODUCTION

Notre société a connu depuis quelques décennies de grands changements, la révolution numérique a bouleversé nos vies, le nombre de personnes connectées[1] est en augmentation constante et l'omniprésence de l'informatique provoquée par des évolutions technologiques permanentes ont propulsé au cœur du débat la question de la protection des données à caractère personnel.

Ces nouvelles technologies posent de nombreuses questions sur l'avenir de la vie privée et entrainent une augmentation non négligeable du volume des collectes et des échanges de données à caractère personnel.

La commission européenne a publié le 25 janvier 2012 une proposition de règlement général sur la protection des données[2], ce projet de règlement a pour objectif le renforcement des droits des citoyens et la modernisation du cadre juridique existant permettant à l'Europe de faire face à l'essor du numérique et à la mondialisation. Cette réforme vise également à aligner le cadre juridique des différents pays membres.

L'article 23 du projet de règlement intègre la prise en compte de la protection des données dès la conception ainsi que la protection des données par défaut reprenant certains aspects du concept de Privacy by Design reconnu à l'échelle internationale depuis 2010 comme une nouvelle norme mondiale par l'«International Association of Privacy Professionals» permettant de compléter un cadre juridique insuffisant.

Le Privacy by Design a pour vocation première d'anticiper toutes les dérives potentielles et les risques d'exploitations abusives des données. Ce concept de Privacy by Design est une réponse.

Synonyme de nouvelles obligations pour les responsables de traitement et de nouvelles missions pour le futur «Data Protection Officer[3]», l'article 23 place ce dernier au centre de chaque ouverture de projet. Le DPO devra rédiger des études d'impact sur la vie privée et s'assurer de la mise en application du concept

La problématique principale de cette thèse professionnelle repose sur le fait de savoir dans quelles mesures les principes fondamentaux pourront être respectés et mis en œuvre de façon optimale pour que tout organisme qu'il soit privé ou public puisse répondre aux nouvelles exigences introduites afin d'être en conformité avec le nouveau cadre juridique européen.

[1] Selon les dernières chiffres communiqués par l'UIT (Union Internationale des Télécommunications), le monde comptait 2,749 milliards d'internautes au premier trimestre 2013 soit 38,8 % de la population mondiale.

[2] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

[3] Le Data Protection Officer est le Correspondant à la Protection des Données à Caractère Personnel » ou de CIL (Correspondant Informatique et Libertés) que l'on connait aujourd'hui, une fois le règlement adopté on parlera du DPO.

Dans une première partie, nous présenterons ce concept de Privacy by Design. Nous analyserons son origine, sa vocation, les principes qui s'y rattachent, les différents secteurs d'activité où le concept a déjà été mis en œuvre, les principaux domaines d'application en étude, sa reconnaissance à travers le monde, ainsi que les nouvelles obligations liées à l'article 23 du règlement européen pour l'entreprise comme pour le DPO.

Dans un second temps nous effectuerons une vue d'ensemble des mesures organisationnelles et des dispositifs techniques qui s'offrent à nous, nous verrons comment les mettre en place en nous appuyant sur des exemples de notre propre expérience professionnelle.

In fine, nous étudierons les innovations et les prospectives possibles du concept dans les années futures. Cela nous permettra d'imaginer des mises en œuvre à un niveau supérieur.

CHAPITRE 1 - UNE DEMARCHE ETHIQUE

Certains en parlent comme d'une approche, un concept prometteur, un ensemble de principes ou encore un article du futur règlement européen. Nous considérons qu'il représente bien plus.

Dans ce premier chapitre nous présenterons le concept de Privacy by Design, les différents éléments liés à sa reconnaissance et les nouvelles obligations concernant sa mise en application dans le cadre de l'article 23 du règlement européen.

1. PRIVACY BY DESIGN

Nous étudierons dans cette première partie ses origines, sa vocation ainsi que les principes sur lesquels le concept repose. Nous donnerons notre lecture de chaque principe, en précisant à qui revient la responsabilité de son application.

1.1. Les origines du concept

Ce concept fut créé au Canada dans les années quatre vingt dix par Ann CAVOUKIAN Ph.D[4]. dans le cadre de ses fonctions de Commissaire à l'information et à la protection de la vie privée de l'Ontario.

À cette époque la protection des données à caractère personnel n'était pas encore une notion synonyme d'enjeu économique. Portée par la défense des libertés fondamentales de l'individu, Ann CAVOUKIAN présente ce concept de Privacy by Design comme une démarche qui vise à assurer la protection de la vie privée.

À l'origine du concept de Privacy by Design on trouve les «technologies renforçant la protection de la vie privée» (PET, Privacy Enhancing Technologies). Le Privacy by Design est une évolution des PETs.

Au cours du séminaire «Respect de la vie privée dès la conception[5]» qui se tenait à Madrid le 2 novembre 2009 le contrôleur européen de la protection des données Peter HUSTINX nous

[4] Ann CAVOUKIAN, Ph.D. est titulaire d'une maîtrise et d'un doctorat en psychologie de l'Université de Toronto où elle s'est spécialisée en criminologie et en droit. Elle est aujourd'hui reconnue comme étant l'un des principaux experts de la protection de la vie privée dans le monde. En octobre 2005, la commissaire CAVOUKIAN s'est vu décernée par l'Association Internationale des Professionnels de la protection de la vie privée (IAPP) le Prix de l'innovation en matière de protection de la vie privée (*Privacy Innovation Award)* au congrès des professionnels de la vie privée le plus important jamais tenu.

Ann CAVOUKIAN est le premier commissaire à l'information et à la protection de la vie privée de l'Ontario à remplir trois mandats. Nommée pour la première fois en 1997, elle supervisera l'application des lois sur l'accès à l'information et la protection de la vie privée jusqu'en 2014.

précise que ce terme de PET est apparu pour la première fois en 1995 dans le rapport «Technologies renforçant la protection de la vie privée : le chemin vers l'anonymat[6]». Ce rapport était le fruit d'un projet commun mené par les autorités Hollandaises pour la protection des données et le Commissariat à l'information et à la protection de la vie privée de l'Ontario. Ann CAVOUKIAN coté canadien et John BORKING du coté hollandais ont à ce moment joué un rôle-clé. Ils présentaient une nouvelle approche de protection de la vie privée.

Les PETs sont à l'origine du principe de «minimisation des données», c'est sur la base de ce principe que s'est développé ce concept de Privacy by Design.

1.2. Une démarche éthique

L'informatique évolue très vite grâce à des innovations techniques permanentes. Il s'agit d'anticiper toutes les dérives potentielles et les risques d'exploitations abusives des données. Ce concept de Privacy by Design est une solution qui nous permettra d'y faire face.

La notion est traduite en français par la protection intégrée de la vie privée (PIVP), ou encore par la prise en compte de la vie privée dès la conception par le Commissariat à l'information et à la protection de la vie privée de l'Ontario.

Cette démarche permet de réaliser des projets informatiques en conformité à Loi Informatique et Libertés de 1978 modifiée en 2004[7] afin de protéger les données à caractère personnel des personnes concernées par lesdits projets, mais également de protéger le droit à la vie privée adoptée et proclamée par l'Assemblée générale des Nations-Unies dans sa résolution 217 (III) du 10 décembre 1948 dans l'article 12 de la Déclaration universelle des droits de l'homme[8].

«*Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes*»

Cette démarche impose d'intégrer à toute technologie exploitant des données à caractère personnel des dispositifs techniques de protection de la vie privée dès sa conception et de s'y conformer tout le long du cycle de vie des données.

---

[5] Madrid, le 2 novembre 2009 «Respect de la vie privée dès la conception (Privacy by Design): le séminaire définitif» - «Privacy by Design : Tenir les promesses»
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf

[6] Privacy-Enhancing Technologies: The Path to Anonymity
http://www.ipc.on.ca/images/Resources/anoni-v2.pdf

[7] Loi Informatiques et libertés de 1978 modifiée en 2004
http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

[8] Le 10 décembre 1948, les 58 États Membres qui constituaient alors l'Assemblée générale ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot (résolution 217 A (III)).
http://www.un.org/fr/documents/udhr/

La démarche repose sur sept principes fondamentaux, et représente une solution permettant aux technologies d'évoluer sans porter atteinte à la vie privée des individus, une coexistence saine et pérenne du numérique et des individus.

1.3. Les sept principes fondamentaux

Fondée sur le principe selon lequel la protection des données à caractère personnel ne pourrait être assurée par le simple respect du cadre légal parfois en décalage avec les technologies actuelles, d'après le Commissariat à l'information et à la protection de la vie privée de l'Ontario la protection intégrée de la vie privée s'applique à un trio d'applications globales : les systèmes informatiques, des pratiques responsables, la conception des systèmes et l'infrastructure des réseaux.

La protection intégrée de la vie privée repose sur sept principes fondamentaux, qui peuvent s'appliquer à toutes les catégories de données à caractère personnel[9], à toutes les mesures organisationnelles, ainsi qu'à tous les dispositifs techniques nécessaires à leur mise en œuvre. Ces derniers devront être en adéquation avec la sensibilité des données traitées.

Il s'agit de rendre à la personne concernée le contrôle sur ses données. En respectant les sept principes fondamentaux développés par Ann CAVOUKIAN, l'ensemble des entreprises qui traitent des données à caractère personnel pourront alors s'inscrire dans une démarche responsable et durable tout en bénéficiant d'un avantage concurrentiel. On pourrait même considérer cette démarche comme la naissance d'une forme de responsabilité sociétale numérique des entreprises.

Ci-dessous, voici les sept principes fondamentaux publiés en aout 2009[10], ces principes sont suivis de notre lecture personnelle de chacun :

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives

La protection intégrée de la vie privée (PIVP) se caractérise par des mesures proactives et non réactives. Elle consiste à prévoir et à prévenir les incidents d'atteinte à la vie privée avant qu'ils ne se produisent. En effet, la PIVP n'attend pas que des risques pour la vie privée se concrétisent, et elle ne propose aucune solution pour résoudre les cas d'atteinte à la vie privée qui se sont déjà produits. Elle vise plutôt à les prévenir. Bref, la protection intégrée de la vie privée vient avant et non après de tels incidents[11].

Ce principe souligne que le concept de Privacy by Design n'offre aucune solution corrective en cas d'atteinte à la vie privée, sa mise en œuvre doit intervenir dans le cycle de vie d'un projet numérique dès sa conception.

---

[9] La CNIL classe les données à caractère personnel en six catégories :
Les données d'Etat-civil (identité, données d'identification), les données liées à la vie personnelle (habitudes de vie, situation familiale), les données de la vie professionnelle (CV, scolarité formation professionnelle, distinctions), les informations d'ordre économique et financier (revenus, situation financière, situation fiscale), les données de connexion (adress IP, logs) et les données de localisation (déplacements, données GPS, GSM).

[10] Les sept principes fondamentaux
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[11] Les sept principes fondamentaux en français
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-f.pdf

Il s'agit d'anticiper les incidents d'atteinte à la vie privée avant qu'ils ne se produisent, ce premier principe place au premier plan l'importance d'agir en amont.

Ce principe est une forme d'indicateur temporel, il situe dans le temps la place de la protection des données à caractère personnel.

Il révèle la nécessité pour l'équipe dirigeante de l'organisme de s'engager réellement dans la prévention des atteintes à la vie privée.

2. Assurer la protection implicite de la vie privée

On peut être sûr d'une chose : la protection intégrée de la vie privée est implicite. Elle vise à procurer le maximum de vie privée en veillant à ce que les renseignements personnels soient systématiquement protégés au sein des systèmes informatiques ou dans le cadre des pratiques internes. Donc, la vie privée d'un particulier est protégée même si ce dernier ne pose aucun geste, car la protection de la vie privée est intégrée dans le système, implicitement.

Il s'agit d'offrir le maximum de vie privée à l'utilisateur, la protection de la vie privée n'est pas optionnelle, en effet un utilisateur doit bénéficier d'une protection maximale sans aucune intervention de sa part.

La notion de « protection implicite » définit la protection des données à caractère personnel comme une convenance qui vise à protéger l'intérêt individuel de chacun, une forme de savoir-vivre ou de bienséance numérique.

Ce second principe est aujourd'hui connu sous le nom de Privacy by Default et repris à l'alinéa 2 de l'article 23 du projet de règlement européen.

«*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.*[12]»

Il est de la responsabilité des développeurs, des chefs projets et des responsables de programmes de mettre en application ce principe.

[12] Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques

La protection intégrée de la vie privée, comme son nom le suggère, est intégrée dans la conception et l'architecture des systèmes informatiques et des pratiques des organismes; elle n'y est pas greffée après coup. La protection de la vie privée devient donc un élément essentiel des fonctionnalités de base. Elle fait partie intégrante du système, sans porter atteinte à ses fonctions.

Ce principe définit la protection de la vie privée comme un élément à intégrer dans la conception et l'architecture même des systèmes informatiques mais également dans les pratiques des organismes.

La protection des données à caractère personnel doit être une composante intégrante du système et de la stratégie organisationnelle de l'organisme sans pour autant porter atteinte à ses fonctions principales.

Pour une application optimale du second principe fondamental, il sera de la responsabilité des développeurs, des chefs projets et des responsables de programmes ainsi que du responsable de la conformité de mettre en application ce principe.

4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle

La protection intégrée de la vie privée vise à tenir compte de tous les intérêts et objectifs légitimes en cause selon un paradigme à somme positive et non selon une approche périmée à somme nulle, qui nécessite des compromis inutiles.
La protection intégrée de la vie privée évite ces fausses dichotomies, par exemple celle qui oppose la protection de la vie privée à la sécurité, en démontrant qu'il est vraiment possible de réaliser ces deux objectifs à la fois.

Ce principe a pour vocation d'imposer une mise en œuvre du concept de Privacy by Design sans porter atteinte au business, en tenant compte de tous les intérêts et objectifs légitimes de l'organisme. La protection des données ne devra pas prendre le pas sur le bon déroulement des affaires.

Le concept de Privacy by Design n'est pas un adversaire du business, ils sont tous deux partenaires et complémentaires selon un paradigme à somme positive.

La protection intégrée de la vie privée doit être considérée par tous les effectifs de l'organisme et plus particulièrement par la fonction commerciale comme une valeur ajoutée inestimable, elle permet de conserver le paramètre confiance des utilisateurs ou des clients, un élément majeur dans la relation client.

La dichotomie opposant la protection des données à caractère personnel à la sécurité selon un paradigme à somme nulle est une approche erronée du concept. En effet cette vision des choses est restrictive et ne peut être provoquée que par un déni total des responsabilités qui incombent au responsable de traitement.

Il est de la responsabilité des développeurs, des chefs projets, des responsables de programmes et des directeurs commerciaux d'assurer la bonne diffusion de ce principe.

5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements

La protection intégrée de la vie privée, lorsqu'elle est intégrée dans le système avant que l'on ne commence à recueillir les renseignements qu'il contiendra, persiste de façon sécurisée pendant toute la période de conservation de ces renseignements; ainsi, des mesures de sécurité essentielles à la protection de la vie privée sont mises en œuvre du début jusqu'à la fin. Cela permet d'assurer la conservation sécurisée des données, puis leur destruction sécurisée à la fin de leur période de conservation. Ainsi, la protection intégrée de la vie privée assure une gestion intégrale, sécurisée et de bout en bout des renseignements pendant toute leur période de conservation.

Ce principe impose d'assurer la sécurité de l'information tout au long de son cycle de vie, on parle alors d'une gestion intégrale visant à garantir une conservation sans risque pour les données et d'en assurer la destruction à la fin de la période de conservation.
La mise en application de ce principe devra être sous la responsabilité du Data Protection Officer ainsi que de toutes les équipes de développement informatique. Le respect de ce principe permettra également d'être en conformité avec l'article 14 du règlement européen.

6. Assurer la visibilité et la transparence

Grâce à la protection intégrée de la vie privée, tous les intervenants seront assurés que sans égard aux pratiques ou aux technologies employées, le système fonctionne conformément aux promesses et aux objectifs établis, sous réserve d'une vérification indépendante. Les éléments et le fonctionnement du système demeurent visibles et transparents, tant pour les utilisateurs que pour les fournisseurs. La vérification permet d'établir un climat de confiance.

Le respect de la vie privée dès la conception garantit au responsable de traitement que le système fonctionne conformément aux promesses et aux objectifs établis.

Chacun des éléments intégrés aux systèmes inhérents à la protection des données à caractère personnel doit rester visible et transparent en cas de vérification indépendante, ce principe vise à conserver un haut climat de confiance. Nous étudierons dans le second chapitre l'ensemble des mesures à mettre en œuvre.

La mise en application de ce principe devra être sous la responsabilité du «Data Protection Officer» ainsi que de toutes les équipes de développement informatique, chefs projets, responsables de programmes et tous les architectes des systèmes d'information. Le DPO sera le mieux placé pour anticiper les attentes de transparence, en effet il sera lui-même amené à effectuer des audits internes, et à répondre en cas de contrôle de la CNIL.

7. Respecter la vie privée des utilisateurs

Avant tout, la protection intégrée de la vie privée oblige les concepteurs et utilisateurs à privilégier les intérêts des particuliers en prévoyant notamment des mesures strictes et implicites de protection de la vie privée, des exigences appropriées quant aux avis et des fonctions habilitantes et conviviales, axées sur l'utilisateur.

Ce principe impose aux concepteurs qui développent le projet et aux utilisateurs qui seront amenés à utiliser le projet une fois développé, de toujours privilégier les intérêts du particulier c'est-à-dire des personnes concernées par les données gérées via le projet ou y ayant accès via webservice. Le principe place la protection des données à caractère personnel de l'utilisateur au centre de toutes réflexions.

Ce principe n'est pas indépendant, il est entrelacé aux six autres, il impose aux concepteurs de munir les systèmes ou les produits qu'ils développent d'une certaine «adequacy[13]», conforme aux attentes des utilisateurs et aux exigences légales.

Comme dans le second principe on peut y voir une forme de savoir-vivre ou de bienséance numérique qui doit être présente au sein du système, ce principe nécessite l'engagement de tous les effectifs de l'organisme.

1.4. Privacy by Design Application Areas

Le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario a publié en décembre 2012 le document «Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices[14]», un condensé d'exemples réels d'organismes et de particuliers qui ont mis en œuvre ce concept de Privacy by Design. Cet ouvrage recense les expériences d'organismes d'un éventail de secteurs d'activité, notamment les télécommunications, la technologie, les soins de santé, le transport et l'énergie.

Il permet ainsi d'avoir une vue d'ensemble de la mise en œuvre du concept dans neuf domaines d'application :

- la vidéosurveillance dans les réseaux de transport en commun
- la biométrie dans les casinos et les établissements de jeu
- les compteurs intelligents et les réseaux électriques intelligents
- les appareils mobiles, les communications sans contact et le RFID
- la géolocalisation par IP
- les consultations médicales à distance
- le Big Data et le Datamining

Dans le cadre de cette thèse professionnelle nous nous limiterons à étudier le trio d'applications globales : la protection intégrée de la vie privée au sein des systèmes informatiques, des pratiques responsables, et via la conception des systèmes et l'infrastructure des réseaux.

En effet un grand nombre de documents ont été publiés sur le concept. Or, aucun ne traite de la mise en œuvre de ce trio d'applications globales qui devrait pourtant être aujourd'hui un socle sur lequel les acteurs du numérique au sein de l'organisme pourraient s'appuyer.

[13] adequacy est un terme qui est le résultat de la concaténation d'«adéquate» et de « privacy», il définit le niveau de conformité adéquate aux attentes européenne et aux CNILs

[14] Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices http://www.privacybydesign.ca/index.php/paper/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/

2. VERS LA RECONNAISSANCE JURIDIQUE D'UN PARADIGME

Dans cette seconde partie, nous reviendrons sur le soutien que le contrôleur européen de la protection des données Peter HUSTINX porte à l'approche Privacy by Design, sur sa reconnaissance comme norme internationale suite à l'adoption d'une résolution historique lors de la conférence internationale à Jérusalem. Nous analyserons par la suite les facteurs auxquels le concept a pu être confronté.

2.1. Un soutien originel de l'Union Européenne

C'est une recommandation du parlement européen à l'attention du Conseil des ministres sur le renforcement de la sécurité et des libertés fondamentales sur Internet publiée le 26 mars 2009 qui marque pour la première fois l'engagement et le soutien de l'Europe dans la promotion du concept de Privacy by Design.

« la protection des données et de la vie privée devrait être introduite dès que possible dans le cycle de vie des nouveaux développements technologiques, assurant aux citoyens un environnement convivial[15]»

En mai 2010 la prise de position de Peter HUSTINX, contrôleur européen de la protection des données, sur la nécessité d'intégrer les principes de Privacy by Design dans les technologies de l'information et de la communication marque à son tour un tournant décisif dans la reconnaissance juridique du paradigme[16].

Peter HUSTINX a par la suite exprimé une nouvelle fois son engagement lors d'une conférence au Parlement européen le 15 novembre 2010 relative à la stratégie de réforme de la protection des données adoptée par la commission le 4 novembre 2010 intégrant le paradigme déjà présent dans le considérant 46 de la directive du 24 octobre 1995 comme un *«élément essentiel de la protection fondamentale de la vie privée*».

Le contrôleur européen de la protection des données Peter HUSTINX souligne que le cadre juridique actuel impose déjà l'obligation de mettre les PET en application via le considérant 46 et l'article 17 de la 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.[17]

Il est intéressant de noter l'absence totale de transposition du considérant 46 et de l'article 17 dans la loi Informatiques et Libertés de 1978 modifiée en 2004 suite à la Directive.

---

[15] Recommandation du parlement européen à l'attention du Conseil des ministres sur le renforcement de la sécurité et des libertés fondamentales sur Internet publiée le 26 mars 2009 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:117E:0206:0213:FR:PDF

[16] Newsletter du CEPD https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_24_FR.pdf

[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 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

La proposition de règlement sur la protection des données publiée par la commission européenne le 25 janvier 2012 a vocation de mettre à jour la Directive 95/46CE[18] et la directive 2002/58CE[19].

Dans le cadre du colloque financé par l'Agence Nationale de Recherche sur le "Privacy by Design, mettre la technologie au service de la vie privée, enjeux limites et perspectives" du 23 mars 2012, Anne CAMMILLERI, Professeure à Sciences Po Rennes souligne dans sa communication "Le Privacy by Design confronte à la disparition des piliers du Traité de Lisbonne[20]" qu'il s'agit pour ces deux textes de défendre le même équilibre entre l'objectif de protection des données à caractère personnel et la libre circulation de ces mêmes données.

Le règlement européen primant sur le droit national devra permettre un renforcement des droits des citoyens et une modernisation du cadre juridique existant. Une fois adopté, il donnera les moyens à l'Europe de faire face à l'essor du numérique et à la mondialisation.

L'article 23 du projet de règlement publié le 25 Janvier 2012 intègre la prise en compte de la protection des données dès la conception et la protection des données par défaut, ces deux notions reprennent certains aspects du concept de Privacy by Design. En effet, elles correspondent au premier et au second principe publiés en août 2009 par le bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

En France, un rapport du groupe «Droit à l'oubli[21]» de Cyberlex publié le 25 mai 2010 a encouragé la mise en œuvre du concept.

Puis un rapport de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique prévoyant une orientation du pays visant à considérer le paradigme comme un atout majeur pour l'Europe et la France[22] a été publié le 22 juin 2011.

[18] 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 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

[19] DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:fr:PDF

[20] Le Privacy by Design confronte à la disparition des piliers du Traité de Lisbonne publié par Anne CAMILLERI
http://www.ceric-aix.univ-cezanne.fr/fileadmin/CERIC/Documents/manifestations_scientifiques/Atelier_Privacy_by_design/cammilleri_privacy_by_design__2_.pdf

[21] Rapport du groupe «Droit à l'oubli[21]» de Cyberlex publié le 25 mai 2010
http://www.cyberlex.org/page-accueil/cyberlex-remet-son-rapport-droit-a-loubli.html

[22] Rapport de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique du 22 juin 2011
http://www.assemblee-nationale.fr/13/rap-info/i3560.asp

2.2. Une reconnaissance internationale

En octobre 2010, le concept de Privacy by Design a été reconnu comme norme internationale de protection de la vie privée suite à l'adoption à l'unanimité d'une résolution historique lors de la conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu à Jérusalem[23].

Le concept a ainsi été reconnu comme un outil de protection de la vie privée à mettre en place pour faire face aux défis futurs. Il s'agit d'une garantie pour l'avenir, cela permet d'assurer que la protection de la vie privée soit intégrée dans les nouvelles pratiques technologiques et commerciales dès la conception.

Cette résolution a pour vocation d'encourager l'adoption des principes du respect de la vie privée dès la conception comme mode de fonctionnement de base des organisations, d'inviter les commissaires à la protection des données et de la vie privée à promouvoir le concept et inciter l'incorporation de ses principes fondamentaux dans les politiques et textes de lois au niveau international.

2.3. Privacy by design aux Etats-Unis

Aux Etats-Unis on peut constater une certaine ambivalence sur la position du gouvernement concernant le concept de Privacy by Design.

En 2011 la Federal Trade Commission[24] des États-Unis a publié un rapport mentionnant le Privacy by Design comme la principale des trois pratiques recommandées pour la protection des consommateurs dans l'économie numérique.

Le 21 mars 2012 à l'European Institute de Washington, Daniel WEITZNER, adjoint en charge de la technologie pour la Politique Internet de la Maison Blanche, a indiqué que le Privacy by Design n'avait pas sa place dans le Livre blanc sur le respect des données que le président OBAMA avait présenté le 23 février 2012.

En effet, selon le haut conseiller, le président Barack OBAMA ne soutient pas le paradigme[25].

Puis en février 2013 la Federal Trade Commission a publié un rapport[26] qui a souligné les principaux enjeux pour les consommateurs et les entreprises de services de paiement mobiles, remettant le concept au cœur du débat. Le rapport contient en effet plusieurs

[23] Résolution historique lors de la conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu à Jérusalem. http://www.justice.gov.il/NR/rdonlyres/3FB67FDB-92DF-4DA0-9146-371DC1992F25/26502/ResolutiononPrivacybyDesign.pdf

[24] La Federal Trade Commission (FTC) est une agence indépendante du gouvernement des États-Unis, créée en 1914 par le Federal Trade Commission Act. Sa mission principale est l'application du droit de la consommation et le contrôle des pratiques commerciales anticoncurrentielle tels que les monopoles déloyaux.
La création de la FTC fut l'une des principales actions du président Woodrow Wilson contre les trusts.
http://fr.wikipedia.org/wiki/Federal_Trade_Commission

[25] Obama ne soutient pas le concept « privacy by design » Par Brian Beary à Washington le jeudi 22 mars 2012http://www.europolitique.info/obama-ne-soutient-pas-le-concept-privacy-by-design-art329724-9.html

[26] Présentation de la FTC : Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments http://www.ftc.gov/os/2013/03/130306mobilereport.pdf

recommandations, notamment en encourageant l'utilisation d'une approche Privacy by Design pour les entreprises développant des applications de paiement mobile[27].

En novembre 2013 Edith Ramirez, la Présidente de la Federal Trade Commission a déclaré qu'étant donné le potentiel d'une nouvelle explosion de la collecte des données de consommation au cours des prochaines années provoquée par l'internet des objets. Les entreprises de ce secteur doivent respecter trois principes fondamentaux adoptés par la FTC : la prise en compte de la vie privée dès la conception, être transparent avec les consommateurs sur la finalité des informations collectées et donner aux consommateurs le contrôle de leurs données[28].

Il sera donc intéressant de suivre les futures positions de la Maison Blanche suite aux diverses révélations d'Edward SNOWDEN[29]. En effet ces révélations ont provoqué des répercutions diplomatiques dans le monde entier[30] et ont une fois de plus éveillé une prise de conscience des citoyens des différents pays visés sur l'importance de la protection de leur vie privée.

---

[27] Federal Trade Commission recommends a Privacy by Design approach for mobile payment services http://www.privacybydesign.ca/index.php/federal-trade-commission-recommends-a-privacy-by-design-approach-for-mobile-payment-services/

[28] FTC Chief : Privacy Principles Should Govern 'Internet of Things' from Privacy & Data Security Law Resource Center http://www.bna.com/ftc-chief-privacy-n17179880336/

[29] Edward Joseph Snowden, est un informaticien américain né le 21 juin 1983, ancien employé de la CIA et de la NSA ,qui a révélé les détails de plusieurs programmes de surveillance de masse américains et britanniques.
À la suite de ses révélations, Edward Snowden est inculpé le 22 juin 2013 par le gouvernement américain sous les chefs d'accusation d'espionnage, vol et utilisation illégale de biens gouvernementaux.
Exilé à Hong Kong en juin 2013, puis à Moscou, Edward Snowden a obtenu le 31 juillet 2013 l'asile temporaire en Russie. http://fr.wikipedia.org/wiki/Edward_Snowden

[30] Comment les révélations d'Edward Snowden ont touché le monde entier, un article de Pauline Hofmann, publié le 20/08/2013
http://www.francetvinfo.fr/monde/espionnage-d-internet/comment-les-revelations-d-edward-snowden-ont-touche-le-monde-entier_393730.html

2.4. 25 ans de leadership (Notes d'Ann CAVOUKIAN)

Suite à nos divers échanges avec le commissariat de l'Ontario au Canada, nous avons souhaité qu'Ann CAVOUKIAN puisse nous donner à la fois son ressenti concernant l'intégration du Privacy by Design dans le règlement européen et également sa vision actuelle du concept. Voici ce qu'elle nous a répondu.

Ann CAVOUKIAN, Ph.D.
Commissaire à l'information et à la protection de la vie privée
Ontario, Canada

Depuis que je l'ai créé dans les années 1990, le concept de *protection intégrée de la vie privée* (*PIVP*) est reconnu de plus en plus comme une démarche permettant d'exercer un meilleur contrôle sur ses renseignements personnels et leur circulation, tout en conférant un avantage concurrentiel durable aux organisations qui y recourent. Par exemple, en 2010, l'association internationale des organismes de protection des données et des commissaires à la protection de la vie privée a adopté à l'unanimité une résolution reconnaissant la *PIVP* comme un élément essentiel de la protection fondamentale de la vie privée. La même année, la Federal Trade Commission des États-Unis a publié un rapport mentionnant la *PIVP* comme première de trois pratiques recommandées. En 2012, l'Union européenne a proposé l'adoption d'un nouveau règlement général sur la protection des données, l'Article 23, qui reprend certains aspects de la *PIVP* et fait l'objet de la présente thèse de mastère. Plus récemment, en 2013, l'Organization for the Advancement of Structured Information Standards (OASIS) a entamé des travaux visant à normaliser les méthodes permettant aux ingénieurs en logiciel d'appliquer les principes de la *PIVP* tout au long du cycle de réalisation des logiciels.
Nos réalisations sont nombreuses mais il reste beaucoup à faire. Les réseaux évolués, les technologies de l'information et des communications et la surveillance accrue menacent de plus en plus notre vie privée de manières nouvelles qui échappent parfois à la portée de la réglementation en vigueur. L'avenir de la protection de la vie privée nécessite un changement de paradigme. Le modèle à somme nulle qui prévaut de nos jours, et qui sacrifie la vie privée à d'autres intérêts, doit être remplacé par un modèle inclusif à somme positive, qui permet de mieux protéger la vie privée tout en tenant compte de facteurs de sécurité ou d'intérêts commerciaux.
J'ai toujours dit que la vie privée est synonyme de liberté. Notre droit de regard sur la collecte, l'utilisation et la divulgation des renseignements qui nous concernent représente l'assise de nos libertés : la liberté d'association, de mouvement et surtout, la liberté de choix - celle de vivre comme bon nous semble.

---

3. ARTICLE 23 : PROTECTION DES DONNEES DES LA CONCEPTION

Dans cette troisième partie nous analyserons l'article 23 et ses évolutions dans la version consolidée de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen, nous verrons ensuite les nouvelles obligations à prendre en compte et le rôle du DPO dans la mise en application du concept.

3.1. L'évolution de l'article 23 du projet de règlement

L'article 23 définit les obligations du responsable du traitement qui découlent des principes de protection des données dès la conception et de protection des données par défaut.

Protection des données dès la conception et protection des données par défaut

1. Compte 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.

2. 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.

3. 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.

4. 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.

Extrait de la proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) du 25 janvier 2012.

L'article 23 du projet de règlement publié le 25 Janvier 2012 intègre la prise en compte de la protection des données dès la conception et la protection des données par défaut, ces deux notions reprennent certains aspects du concept de Privacy by Design. En effet, le premier alinéa et le second alinéa correspondent respectivement au premier et au second principe publiés en août 2009 par le bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

L'article 23 a également pour objectif d'imposer au responsable de traitement l'intégration du concept dans son système d'information et dans son infrastructure, cette nouvelle obligation quant à elle correspond au troisième principe fondamental.

De prime abord, il semblait regrettable d'avoir limité l'intégration du paradigme à seulement trois principes fondamentaux. Cependant, la raison de cette limitation pouvait s'expliquer d'une part, par le fait que l'intégration complète des sept principes aurait pu provoquer certaines redondances législatives dans le cadre juridique européen et d'autre part, par la lourdeur que la notion aurait comporté, risquant ainsi une exclusion totale.

Dans sa forme originelle l'article 23 laissait la porte ouverte à une multitude de nouvelles notions. Les alinéas 3 et 4 offraient la possibilité d'intégrer de nouveaux principes, une fois l'adoption définitive du règlement européen l'interprétation de l'article 23 par des juges ou l'introduction d'actes délégués en conformité avec l'article 86 du projet de règlement auraient pu préciser d'éventuels critères et exigences supplémentaires. Ils avaient tous les deux vocation de donner au concept les moyens d'évoluer.

Suite aux modifications publiées dans la version consolidée[31] de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen menée par Jan Philipp Albrecht, les éléments suivants ont été intégrés :

Nous avons pu constater que le premier alinéa a été enrichi de manière conséquente, il est maintenant relié aux articles 5 et 33 qui reprennent un grand nombre de notions.

Des notions comme :

- la transparence,
- la finalité de traitement,
- l'intégrité des données,
- l'adéquation des mesures et des dispositifs mis en place,
- ainsi que le respect des durées de conservation sont présents dans l'article 5.

L'article 33 quant à lui reprend l'ensemble des éléments dont les études d'impact devront être composées.

Des notions comme :

- la protection des données tout au long du cycle de vie,
- l'intérêt légitime poursuivi,
- la proportionnalité,
- l'archivage,
- l'anonymisation,
- l'encadrement des flux transfrontaliers,
- la protection des données dès la conception

[31] La version consolidée[31] de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen menée par Jan Philipp Albrecht http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

- et l'implication du DPO sont des éléments que l'article 33 impose de prendre en compte lors de la rédaction d'une étude d'impact.

On retrouve donc la transparence et la protection des données tout au long du cycle de vie qui correspondent respectivement au sixième et au cinquième principe publiés en août 2009 par le bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.
L'alinéa 1a a aussi fait son apparition, il impose à toutes institutions publiques l'obligation de mettre en œuvre le concept Privacy by Design à toutes initiatives de projet collectant des données à caractère personnel.

Nous avons également pu constater la suppression complète des alinéas 3 et 4 suite aux modifications publiées dans la version consolidée de la proposition du règlement européen après le vote LIBE du 22 octobre 2013.

Face à toutes ces évolutions, nous avons pris contact avec Jan Philipp Albrecht afin d'obtenir sa vision sur toutes ces évolutions.

Nous lui avons donc demandé dans quelles mesures toutes ces modifications représentent une avancée pour le développement du concept. Et, si la suppression des alinéas 3 et 4 était bien une stratégie visant à protéger l'article 23 modifié de futurs actes délégués qui auraient pu restreindre a posteriori son champ d'application ou exclure certains secteurs d'activité.

Voici ce qu'il nous a répondu :

Jan Philipp Albrecht considère que les modifications apportées améliorent l'article 23, en effet l'obligation d'intégrer le concept dans tout système d'information et dans toute infrastructure jusque-là implicite est maintenant bien plus clair que dans la première version de proposition. L'apparition de l'alinéa 1a imposant l'application du Privacy by Design pour l'obtention de marchés publics a vocation de créer un marché durable pour des produits et des services favorables à la protection de la vie privée.

L'effacement des alinéas 3 et 4 quant à lui fait partie d'un effort général qui vise à diminuer le nombre d'actes délégués pouvant être ajoutés a posteriori. En effet Jan Philipp Albrecht estime que la commission européenne n'a pas vocation de codifier des normes techniques.

3.2. Les nouvelles obligations à prendre en compte

En plus de tout ce qui a été précisé précédemment, l'article 23 introduit également de nouvelles obligations pour les responsables de traitements.

L'implication du «Data Protection Officer» est maintenant imposée pour tous projets devant intégrer le concept de Privacy by Design. Le DPO devra donc avoir une réelle maitrise des dispositifs techniques et des mesures organisationnelles afin d'être consulté ab initio.

Le «Privacy Impact Assessment» est également une nouvelle obligation introduite par le bais de l'article 33 du règlement européen. L'étude d'impact de vie privée a vocation d'évaluer les risques d'atteinte à la vie privée et leur impact sur les personnes concernées. Elle devra décrire toutes les mesures mises en œuvre par l'organisme pour y faire face.

Dans la pratique ces études d'impact devront être réalisées avant la mise en place du paradigme, destinées à justifier l'inscription de l'organisme dans une démarche responsable. Elles représentent aussi pour le DPO un outil performant pour exprimer ses recommandations dès la conception d'un projet.

En septembre 2013 la CNIL a publié un document[32] «COMMENT REALISER UNE EVALUATION D'IMPACT SUR LA VIE PRIVEE (EIVP) POUR LES DISPOSITIFS RFID ?» une présentation générale de la méthodologie européenne permettant de répondre aux attentes de Commission européenne et de la CNIL.

3.3. Le rôle du Data Protection Officer

Le «Data Protection Officer» tiendra un rôle majeur dans la mise en œuvre du concept de Privacy by Design.

L'article 33 précise donc clairement que le DPO devra donc être impliqué à tous projets de développement informatique qui permettront in fine la collecte de données à caractère personnel.

En plus de la rédaction des études d'impact et de se former dans l'optique d'avoir une réelle maitrise des dispositifs techniques et des mesures organisationnelles déjà évoquées précédemment, il devra instaurer la mise en œuvre des différents principes à l'aide de plusieurs schémas organisationnels.

Il lui incombera également la tâche de définir les responsabilités de chacun concernant la protection des données à caractère personnel et d'être en mesure de collaborer avec les différents services de l'organisme.

[32] COMMENT REALISER UNE EVALUATION D'IMPACT SUR LA VIE PRIVEE (EIVP) POUR LES DISPOSITIFS RFID ? http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Methodologie-etude_impact_RFID.pdf

CHAPITRE 2 - LA MISE EN OEUVRE DU CONCEPT

Dans ce second chapitre nous présenterons des mesures organisationnelles et des dispositifs techniques nécessaires pour mettre en application le concept de Privacy by Design. Nous étudierons ensuite plusieurs exemples de «technologies renforçant la protection de la vie privée» (PET, Privacy Enhancing Technologies) et quelques innovations et prospectives liées au concept.

1. SEPT MESURES ORGANISATIONNELLES POUR SEPT PRINCIPES

Voici sept mesures organisationnelles que nous recommandons vivement afin de mettre en œuvre le concept de Privacy by Design au sein d'un organisme qu'il soit public ou privé. Chacune de ces mesures est liée à l'un des sept principes fondamentaux sur lesquels repose le concept. Le cumul de toutes ces mesures conduira l'organisme vers une application optimale du paradigme.

1.1. Une philosophie pour le Data Protection Officer

Respecter le premier des sept principes fondamentaux pour le «Data Protection Officer» est comme une philosophie à appliquer à l'ensemble des situations auxquelles il peut être confronté. Il doit diffuser ce principe dès qu'il est possible de le mettre en œuvre.

En ce qui concerne la «Privacy Impact Assessment», nous recommandons d'imposer la rédaction d'une étude d'impact avant chaque ouverture de projet via la politique de protection des données à caractère personnel qu'il devra mettre en œuvre.

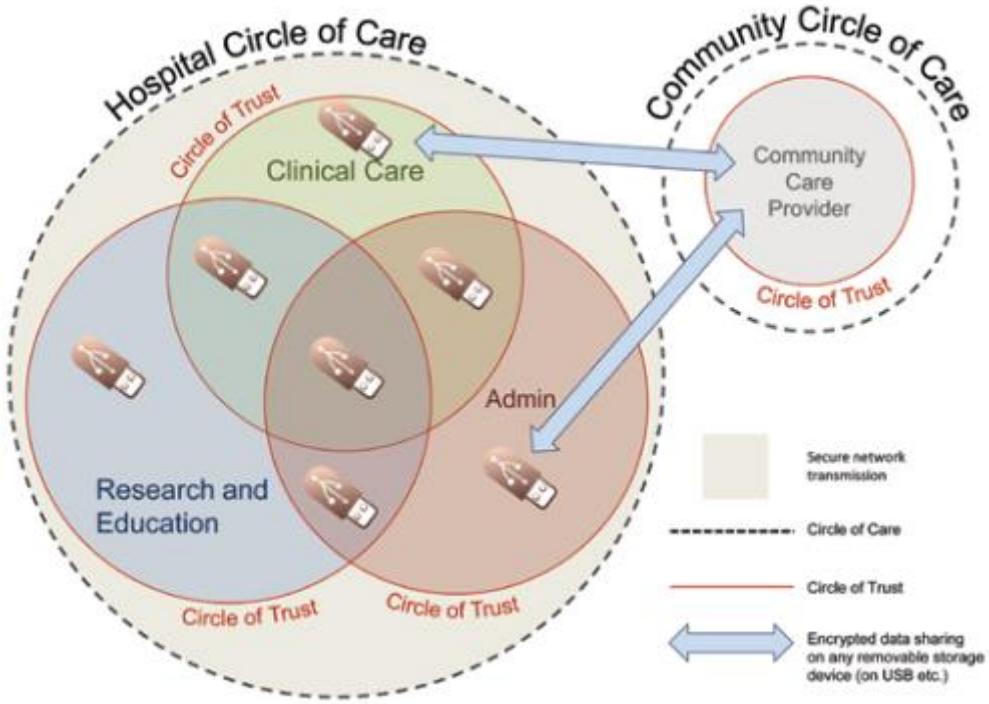
En plus de sa vocation principale, l'étude d'impact de vie privée permettra au DPO de justifier des différentes recommandations établies, de l'ensemble des mesures mises en place et à l'organisme de prouver qu'elle a fait la démarche de mettre en place des procédures proactives. Il s'agit d'anticiper toutes atteintes possibles de la vie privée.

Il faudra appliquer la même philosophie à la gestion et à la création de nouveaux fichiers. Les formalités déclaratives effectuées par les organismes qui n'ont pas désigné de «Correspondant Informatique et Libertés», les fiches de traitements du registre tenu par le CIL désigné ou la documentation que le DPO devra tenir devront être rédigées avant la mise en place effective des fichiers.

1.2. Le chiffrement par défaut et les cercles de confiance : Encryption by Default and Circles of Trust

Voici un modèle d'organisation des cercles de confiance extrait de «Encryption by Default and Circles of Trust : Strategies to Secure Personal Information in High-Availability Environments[33]», publié en décembre 2012 par le bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

Ce document explique comment mettre en place un scénario de déploiement en fonction des différents profils d'intervenants que l'on peut trouver dans un hôpital universitaire.



Cet exemple de déploiement du principe de Privacy by Design permet de tirer les enseignements suivants. Il y a trois cercles de confiance à l'intérieur de l'hôpital, un cercle pour chaque secteur.

L'objectif est de limiter l'accès aux informations qui rentrent dans le cadre de l'activité de l'organisme concerné, en fonction de chaque profil.

Par exemple, un étudiant pourra accéder à toutes les différentes pathologies rencontrées dans l'hôpital dans le cadre de ses recherches sans pour autant avoir accès à des informations qui lui permettraient de relier ces informations avec un patient.

De la même manière, les membres du service d'administration de l'hôpital accèdent aux données personnelles des patients sans avoir accès aux dossiers médicaux, ils accèdent

[33] Encryption by Default and Circles of Trust : Strategies to Secure Personal Information in High-Availability Environments http://www.privacybydesign.ca/content/uploads/2012/12/pbd-circlesoftrust.pdf

également aux données correspondantes aux identités des élèves sans pour autant avoir accès à leurs recherches.

L'hôpital est lui-même un cercle de confiance sécurisé par un cercle de confiance d'hébergeurs et d'informaticiens.

Le cercle de confiance dans lequel se trouve l'ensemble des cercles de confiance peut parfois aussi être sécurisé physiquement via des agents de sécurité.

Ces deux stratégies sont étroitement liées au second principe fondamental. En effet le «Privacy by default» a pour objectif de répondre à ce besoin de confidentialité en fonction des différentes situations, comme le secret professionnel dans le secteur de la santé.
Il s'agit d'instaurer une bienséance numérique qui vise à protéger l'intérêt individuel de chacun.
Le chiffrage par défaut et les cercles de confiance sont deux stratégies dont le but est de garantir la protection des données à caractère personnel dans des environnements de haute disponibilité. Ces deux stratégies ont été mises en place simultanément pour la première fois dans le secteur de la santé par la société CryptoMill Technologies

Il est possible de mettre en place ce genre de scénario dans une multitude de secteurs, on peut retrouver ce type d'organisation d'accès en fonction des profils dans des ministères, des entreprises d'aéronautique, ou encore dans certains centres de données.

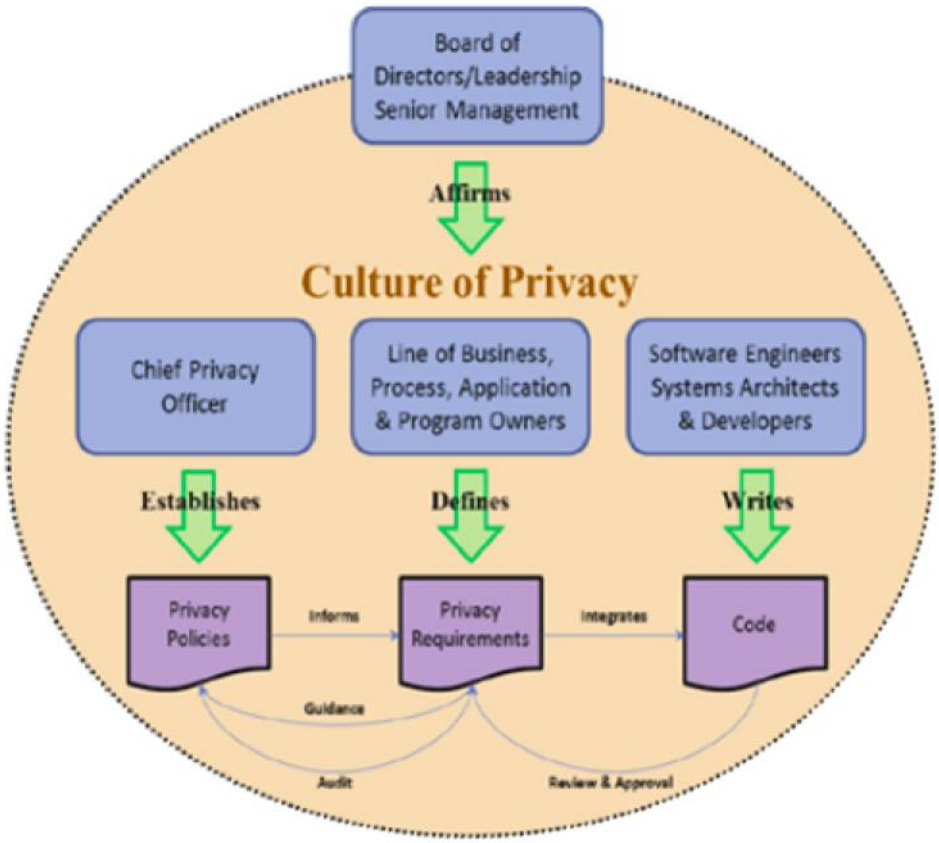
1.3. Développement d'une culture « Privacy »

Le premier pré requis indispensable à la mise en œuvre optimale du Privacy by Design est le développement d'une culture «Privacy» au sein de l'organisme concerné.
Si une entreprise ou un organisme souhaite s'inscrire dans une démarche responsable et durable, il est impératif que l'ensemble de son personnel à tous les niveaux hiérarchiques soit mobilisé.

Lorsque l'on parle de protection de données à caractère personnel, chacun d'entre nous à un rôle à jouer, les responsabilités de chacun doivent être clairement délimitées.

Voici un modèle d'organisation des responsabilités inhérentes à la protection des données à caractère personnel extrait de «*Operationalizing Privacy by Design*[34]» publié en décembre 2012 par Ann CAVOUKIAN dans le cadre de ses fonctions de Commissaire à l'information et à la protection de la vie privée de l'Ontario.

[34] Operationalizing Privacy by Design http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf



Ce modèle d'organisation est un élément-clé pour une mise en œuvre optimale du concept de Privacy by Design. Il est applicable à toute taille d'organisme en définissant le rôle de chaque fonction au sein de ce dernier.

À titre de remarque, plusieurs éléments sont étroitement liés à certains des sept principes fondamentaux.

Pour une intégration organisationnelle optimale du Privacy by Design, plusieurs actions doivent être mises en place:

- L'équipe dirigeante doit affirmer son engagement pour que l'organisme dans son ensemble puisse s'inscrire dans une démarche responsable, l'objectif est de placer l'organisme dans une position de conformité adéquate aux attentes européennes.

- Le Data Protection Officer ou la personne chargée de la protection des données doit établir une politique de protection des données à caractère personnel reprenant les sept principes du concept de Privacy by Design. La politique de protection n'a donc pas vocation de définir quelles seront les données collectées, mais plutôt quelles mesures et quelles pratiques devront être mises en place afin d'en assurer la sécurité.

- Les effectifs de l'organisme devront respecter ladite politique de protection des données à caractère personnel.

- La direction commerciale et les responsables de programme devront définir l'ensemble des données à caractère personnel nécessaires au développement optimal des affaires, chacune des finalités devront être définies au sein d'une charte de protection des données personnelles.

- Les architectes des systèmes d'information, les ingénieurs logiciels et les développeurs auront pour mission d'intégrer lors de l'écriture du code toutes les exigences décrites dans la politique rédigée par le DPO et par la charte de protection des données personnelles mise en place par les équipes commerciales.

1.4. « Privacy is good for business »

La protection intégrée de la vie privée doit être considérée comme une valeur ajoutée inestimable dans les fonctions commerciales et mercatiques de l'organisme.

La dichotomie opposant la protection des données à caractère personnel à la sécurité selon un paradigme à somme nulle est une approche erronée du concept, en effet le respect de la vie privée permet d'augmenter et de conserver le paramètre confiance des utilisateurs ou des clients, un élément majeur dans la relation client[35].

Pour l'organisme, en plus de satisfaire ses besoins en conformité, la mise en œuvre de pratiques et de mesures proactives permettra d'exclure les éventuels coûts liés aux conséquences financières entrainées par de potentielles atteintes à la vie privée.

[35] Operationalizing Privacy by Design http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf

En effet suite à une atteinte à la vie privée, un organisme peut être confronté à de multiples problématiques.

Les principales conséquences possibles sont :

- Les coûts liés à une mise en place imposée a posteriori.
- Les poursuites judiciaires des clients ou des autorités de protection des données.
- Une perte du paramètre confiance de l'utilisateur ou du client.
- Des dommages sur l'image de la marque ou de l'organisme qu'elle représente.

Il faut souligner que les investissements liés à une mise en œuvre réactive, la perte du paramètre confiance et les dommages sur l'image de la marque pourront entrainer des coûts difficilement mesurables. Les coûts des poursuites judiciaires jusqu'à présent négligeables ont vocation à devenir très importants, la Commission européenne a de son côté proposé des peines allant jusqu'à un million d'euros ou 2% du chiffre d'affaires annuel mondial de l'organisme une fois le règlement adopté.

Une réputation repose sur plusieurs années de travail mais peut s'écrouler bien plus vite. Il est difficile de considérer qu'éviter des coûts peut parfois représenter un gain.

On peut également appliquer le même raisonnement suite à la remise en cause d'un produit ou d'un système non conforme à la réglementation ou ne répondant pas aux nouvelles exigences du marché.

Le concept de Privacy by Design n'est pas un adversaire du business, ils sont tous deux partenaires et complémentaires selon un paradigme à somme positive.

1.5. Modélisation du cycle de vie des données

Nous considérons que la modélisation du cycle de vie des données est un élément-clé dans l'automatisation du respect des durées de conservation.

De nombreux travaux concernant la modélisation du cycle de vie des données existent. La Commission nationale de l'informatique et des libertés recommande d'adopter une politique d'archivage, afin de concilier les besoins d'exploitation des données avec le respect de la vie privée.[36]

La doctrine de la CNIL à ce sujet repose sur trois catégories d'archives définies par le code du patrimoine :

- les archives courantes, par exemple les données relatives à un client dans le cadre d'un contrat.

[36] Guide "Gestion des risques vie privée" Méthodes et catalogue des mesures publié par la CNIL en 2012.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf

- les archives intermédiaires, qui présentent un intérêt administratif pour les services concernés : leur durée de conservation est fixée en fonction des autres textes.
- les archives définitives, qui ont un intérêt strictement historique, scientifique ou statistique : elles peuvent être conservées indéfiniment.

Dans le cadre d'une mise en œuvre optimale du cinquième principe, nous recommandons de choisir ou d'établir un référentiel des durées de conservation des catégories ou des types de données traitées dans le cadre de l'activité de l'organisme.

Il conviendra ensuite d'appliquer le troisième principe en intégrant d'une part, des métadonnées permettant l'identification du niveau de sensibilité des données au cœur du système et d'autre part, une table des durées de conservation retenues au sein de la base de données.

Une fois ces deux mesures mises en place le système pourra agir seul, et sera également un des garants du bon déroulement du cycle de vie des données. Il aura la faculté de choisir quel type d'archivage ou de chiffrement appliquer, et devra offrir la possibilité de détruire les données à supprimer via une simple confirmation à l'ouverture d'une session administrateur.

1.6. Transparence et responsabilité

Il conviendra d'utiliser la même stratégie de cumul des principes pour mettre en œuvre le sixième. L'objectif est la mise en place d'une traçabilité des utilisateurs appartenant aux effectifs de l'organisme.

Nous recommandons de mettre en place une surveillance des différentes actions exécutées. Ce niveau de protection est proportionné, nous considérons qu'il est préférable de surveiller un nombre restreint d'utilisateurs pour assurer la protection d'un grand nombre de clients.

Il sera donc souhaitable de lister l'ensemble des actions possibles, ainsi que le nombre d'itérations autorisées à subir simultanément telle ou telle action afin d'alerter en temps réel les administrateurs d'une utilisation malveillante du système.

Ce système de traçabilité offrira à l'organisme un niveau de transparence adéquate, il pourra en cas de contrôle indépendant présenter un historique de toutes les actions effectuées par ses effectifs, rendre accessible à tous les durées de conservation appliquées par le système.

L'étude d'impact là encore aura un rôle important dans cette volonté de transparence, elle devra aussi bien être disponible pour les autorités de contrôle que pour des clients désireux de s'assurer du niveau de protection de leurs données.

Il faudra aussi souligner qu'appliquer le septième principe offrira un meilleur contrôle à l'utilisateur client sur ses données, l'automatisation du droit d'accès provoquera aussi une augmentation du niveau de transparence.

Toutes ces mesures représenteront l'ensemble des moyens mis en œuvre par l'organisme pour affirmer sa volonté de s'inscrire dans une démarche responsable.

1.7. Une vision centrée sur l'utilisateur

L'intégration du septième principe de Privacy by Design à l'intérieur du système et au sein de l'organisation des effectifs permet de donner un contrôle optimal à l'utilisateur sur ses données, il doit être en mesure d'accéder à toutes les informations le concernant et autorisé à les modifier ou les supprimer.

Dans un monde centré sur l'utilisateur la demande de droit d'accès n'aurait pas lieu d'exister.

Cette notion aura également un grand rôle à jouer au sein de l'article 18 du règlement relatif au droit de portabilité par la suite intégré à l'article 15 quant à lui relatif au droit d'accès. Ce nouveau droit à la portabilité des données paraît être une réelle avancée en matière de protection des données à caractère personnel, il pourrait procurer dans l'avenir à l'utilisateur un meilleur contrôle sur ses données et renversera potentiellement toutes les notions et procédures déjà intégrées ou mises en place par les organismes inhérents au droit d'accès.

Il conviendra donc de s'assurer que le contrôle effectif sur les données personnelles soit uniquement et exclusivement offert à la personne concernée, et ne se transforme pas en une standardisation destinée à normaliser certaines tables qui contiennent des données à caractère personnel présentes dans un grand nombre de bases de données.

En effet, si cette normalisation n'est pas réalisée dans les règles de l'art, c'est-à-dire sans prendre en compte l'ensemble des principes de privacy by design, le risque réside sur les conséquences « Privacide » qui pourraient être provoquées par une utilisation malveillante du datamining.

2. DISPOSITIFS TECHNIQUES

Dans cette seconde partie, nous verrons l'importance de la cryptographie dans la mise en application technique du concept et une méthode permettant d'augmenter le niveau de protection des empreintes de contrôle d'intégrité.

2.1. La cryptologie

Étymologiquement on traduit le terme "cryptologie" comme la science du secret. Cette pratique fut utilisée au cours des différents siècles de l'histoire, déjà en 2000 av. J.-C. les égyptiens cryptaient leurs hiéroglyphes, et par la suite Jules César lui-même communiquait avec ses généraux grâce à un chiffrement par décalage connu aujourd'hui comme "le Chiffre de César[37]".
Ce besoin de limiter l'accessibilité d'une information stratégique à une personne ou encore à un groupe restreint d'individus n'est pas nouveau.

Aujourd'hui lorsque l'on parle de cryptologie, cela regroupe la cryptographie dont l'objectif est de chiffrer un message et la cryptanalyse dont la vocation est l'analyse des différents chiffrements.
La cryptographie se subdivise également en deux types bien distincts :
la cryptographie symétrique dite classique, et la cryptographie asymétrique dite moderne.

La cryptologie ne concernait au début qu'une minorité d'individus, ou d'organisations gouvernementales, comme l'armée ou les services secrets.
C'est pour cette raison qu'il y a encore peu de temps la cryptologie était considérée comme une arme de guerre dans beaucoup de pays y compris les Etats-Unis et la France.

Suite à l'avènement de l'internet, du web dit 2.0, des réseaux sociaux et des smartphones, la cryptographie a aujourd'hui une place fondamentale dans l'économie ainsi que dans notre vie quotidienne.
Ces nouvelles technologies ont entraîné une augmentation non négligeable du volume des collectes et des échanges de données à caractère personnel. Ce phénomène a créé un besoin massif de sécurité et de confidentialité des utilisateurs comme conséquence collatérale.

La cryptologie a longtemps été interdite en France car elle était considérée jusqu'en 1996 comme une arme de guerre de deuxième catégorie.

La législation française s'est par la suite assouplie autorisant le chiffrement symétrique avec des clés ne dépassant pas 128 bits.

Suite à l'apparition des sites de commerce en ligne, la loi pour la confiance dans l'économie numérique du 21 juin 2004[38] a totalement libéré l'utilisation des moyens de cryptographie, en revanche, leur importation ou exportation reste soumise à déclaration ou autorisation.

[37] Chiffrement par décalage : http://fr.wikipedia.org/wiki/Chiffrement_par_décalage
[38] Loi pour la confiance dans l'économie numérique
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id

2.2. La cryptographie un élément clé du Privacy by Design

La cryptographie a un rôle central dans les différents dispositifs techniques à mettre en place afin de protéger des données à caractère personnel.

Il existe deux systèmes de chiffrement, le système de chiffrement symétrique et le système de chiffrement asymétrique.

Le système de chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer alors que le système de chiffrement asymétrique repose sur une paire de clés, une clé publique liée à une clé privée.
Un message crypté par une des deux clés ne pourra être décrypté que par l'autre clé.

Nous verrons que nous utilisons déjà l'ensemble de ces différents systèmes de chiffrement au quotidien afin de répondre souvent à ce besoin d'anticiper toutes les dérives potentielles et les risques d'exploitations abusives de nos données personnelles.

Dans l'optique d'une mise en œuvre du concept de Privacy by Design conforme aux attentes légitimes de l'ensemble des utilisateurs de toute plateforme numérique digne de confiance, il faudra s'assurer que tous les points suivants sont respectés.

Il faut donc intégrer un niveau de sécurité très élevé, sans jamais oublier que le risque zéro n'existe pas en sécurité informatique.

En effet, le nombre d'experts en sécurité informatique à l'abri de tout piratage potentiel victime finalement d'une intrusion sur leur système est lui aussi très élevé.

La pire situation à laquelle une plateforme numérique peut être confrontée mais qui pourtant est un grand basique du piratage se nomme le "dump", l'extraction complète de la base de données.

Le système de chiffrement symétrique est un dispositif technique qui permet de limiter les conséquences collatérales qui peuvent se produire a posteriori.

Les données les plus sensibles comme les coordonnées bancaires d'un client ont l'obligation d'être stockées via un chiffrement symétrique dans les bases de données. En effet, la CNIL exige que les données bancaires soient cryptées par l'intermédiaire d'un algorithme de chiffrement dit "fort"[39].

Il y a différentes méthodes de cryptage symétrique, les trois principales sont le DES, le triple DES et l'AES. Suite aux révélations de l'été 2013, nous recommandons donc de mettre en place un cryptage symétrique avec la méthode AES avec une clé de 256 bits a minima.

---

[39] Fiche pratique : Un site marchand peut-il conserver mes données bancaires ? publié par la CNIL le 21 juin 2011 http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-site-marchand-peut-il-conserver-mes-donnees-bancaires/

Le système de chiffrement asymétrique est un dispositif technique qui peut être utilisé à différents niveaux. Il a un rôle primordial dans la sécurité liée aux navigations sur le web : on peut le rencontrer dans le protocole https.

Le https est un protocole de transfert de fichiers avec une couche de chiffrement TLS qui repose sur un chiffrement asymétrique entre le client et le serveur.
Une des mesures de sécurité appropriée serait donc de mettre en place le protocole https lors de la conception d'une plateforme numérique hébergeant des données à caractère personnel.

Naviguer sur le web via un protocole http non sécurisé revient à se promener nu sur la voie publique : dans le monde numérique, une quantité non négligeable d'individus ont la faculté d'espionner n'importe qui en temps réel.

Le chiffrement asymétrique peut être également utilisé de manière plus basique dans le monde de l'entreprise pour permettre à un contact d'envoyer un message chiffré en s'assurant qu'il ne pourra être déchiffré que par une seule personne. Cette pratique ne pourra être mise en place sans mesure organisationnelle. Il convient donc d'inviter les contacts potentiels à utiliser la clé publique de l'organisme pour s'assurer que seul l'organisme puisse ouvrir un message envoyé.

Dans la cryptographie il existe également le hashage. Ce n'est pas un système, il s'agit de fonctions qui ont vocation à chiffrer une chaine de caractères ou un fichier sans déchiffrement possible. Ces fonctions permettent un contrôle d'intégrité.

Le hashage permet de conserver l'empreinte générée par un mot de passe d'un utilisateur sans jamais en être en possession.

Ce principe est appliqué par exemple dans le secteur de la biométrie grâce auquel il est possible de stocker l'empreinte générée par une donnée biométrique (empreintes digitales, iris, réseaux veineux etc..) sans jamais la conserver en clair.

Le hashage peut également se retrouver dans les "computer forensics", en cas de saisie informatique dans le cadre d'une enquête policière, les officiers de police judiciaire ont l'obligation de générer une empreinte de l'ensemble des fichiers saisis pour assurer qu'aucune altération ou modification ait lieu entre le moment de la saisie et le jugement[40].

Il faudra donc faire appliquer ces trois recommandations pour répondre aux exigences implicites afin d'obtenir le niveau de sécurité nécessaire lors d'une mise en œuvre du concept.

Récapitulons :

- Crypter les données sensibles stockées dans une base de données à l'aide d'un chiffrement symétrique.

[40] Informatique légale : http://fr.wikipedia.org/wiki/Informatique_légale

- Activer le protocole https sans oublier de rediriger le protocole http sur le https pour exclure toute faille de sécurité. La redirection permettra d'éviter toute navigation en clair et potentiellement exposée à certaines DPI "Deep Packet Inspection" (traduit en français par "Inspection des Paquets en Profondeur")
- Il est clairement conseillé de gérer les accès à la plateforme à l'aide d'un contrôle d'intégrité afin de s'assurer qu'aucun n'intervenant quel qu'il soit puisse avoir connaissance des différents mots de passe

2.3. Un contrôle d'intégrité augmenté

Le contrôle d'intégrité est une méthode utilisée pour calculer l'empreinte d'un mot de passe. Cette méthode donne la possibilité au système de stocker l'empreinte du mot de passe sans jamais en avoir connaissance, nous pourrons donc comparer l'empreinte calculée avec l'empreinte stockée pour vérifier qu'elles sont bien identiques.

Nous recommandons vivement de mettre en place un contrôle d'intégrité en utilisant la fonction SHA1, la fonction MD5 étant aujourd'hui obsolète.

Les fonctions de hash sont des fonctions irréversibles, il n'existe pas d'algorithme ou de fonctions permettant de retrouver la chaîne d'origine. La seule solution pour déchiffrer un hash est de chiffrer un ensemble de chaînes de caractères afin de générer un dictionnaire. Ainsi, chaque chaîne cryptée sera comparée au hash recherché jusqu'à trouver la correspondance.

Il existe principalement trois méthodes de déchiffrement par comparaison :

- Le brut force, qui consiste à générer toutes les combinaisons possibles d'une chaîne pour une longueur donnée.
- l'attaque par dictionnaire, qui consiste à utiliser les mots d'un dictionnaire stockés sur un fichier texte.
- Le rainbow table ou table arc-en-ciel qui est en cryptanalyse une structure de données qui a pour vocation de retrouver un mot de passe à partir de son empreinte. L'intérêt de stocker un dictionnaire en base de données est d'augmenter les performances du temps de réponse des requêtes lors d'une attaque. La constitution d'un tel dictionnaire prend du temps et doit être faite à l'avance. Toutefois elle est envisageable.

Il existe également des phénomènes de collisions. On peut parfois constater qu'un couple de données dans son ensemble de départ est tel que leur somme de contrôle est identique.

Afin de répondre à ces différentes problématiques, on utilise la technique du grain de sel qui consiste à introduire un grain de sel qui va déformer le hash attendu. Ce grain de sel est en fait un très grand nombre que l'on concatène au mot de passe avant de le chiffrer.

Cette technique est une évolution de la méthode "Shamir", une méthode incontournable dans la gestion du secret[41]. Cette méthode repose sur l'atomisation d'une clé secrète en

[41] Secret réparti : http://fr.wikipedia.org/wiki/Secret_réparti

plusieurs éléments imposant la présence de plusieurs personnes pour déchiffrer. On peut retrouver l'utilisation de cette méthode dans le secteur bancaire pour accéder à des coffres-forts en effet, un client ne peut accéder à son coffre sans la présence de la clé détenue par la banque.

Il convient donc d'ajouter une valeur au mot de passe avant de le hasher pour s'assurer que le même mot de passe ne donne pas le même hash et limiter les potentiels possibilités de collisions tout en augmentant la protection face à d'éventuelles attaques.
Ainsi au lieu d'enregistrer le hash du mot de passe seul, on peut enregistrer le hash du mot de passe suivi de l'adresse e-mail de la personne ou encore de son login. L'objectif est juste d'augmenter la complexité du hashage.

Prenons un exemple concret :

Le mot de passe de l'utilisateur "alex" est le suivant : "adequacy"
le hash est égal à : sha1("adequacy")

Le hash contient alors ab7022aa0dce0cd0d434c4069ff66966186ed966 qui est le hash de adequacy. Si l'on avait un dictionnaire avec tous les hashs possibles, on pourrait alors associer ab7022aa0dce0cd0d434c4069ff66966186ed966 à adequacy et donc obtenir le mot de passe.

Nous recommandons donc de concaténer le login au mot de passe pour effectuer le contrôle d'intégrité : le hash sera alors égal à : sha1("alexadequacy") qui sera plus difficilement retrouvé dans un dictionnaire et générera également deux chaines différentes pour deux utilisateurs utilisant le même mot de passe.

3. TECHNOLOGIES RENFORCANT LA PROTECTION DE LA VIE PRIVEE (Privacy Enhancing Technologies)

Dans cette troisième partie nous verrons des exemples de «technologies renforçant la protection de la vie privée», ces exemples peuvent être applicables dans tout type d'organisme qu'il soit public ou privé.

3.1. Gestion de messagerie proactive (Privacy Enhancing Strategie's messaging)

Les choix techniques inhérents à l'infrastructure de messagerie sont stratégiques pour la sécurité de l'organisme. Dans la majeure partie des cas, les intrusions, les détournements d'informations ou de clientèles proviennent de personnes internes à l'organisme. Il s'agit de ne jamais perdre le contrôle et anticiper toutes les dérives potentielles.

Pour le DPO, il s'agit de recommander une analyse de risque, car trop souvent la solution la moins onéreuse est celle choisie.

L'analyse de risque permettra aux responsables une réelle prise de conscience des risques potentiels. La messagerie est l'une des formes de communication que l'organisme utilise ; une information partielle, ou l'ensemble du patrimoine informationnel peut ainsi être transféré en quelques secondes.

Dans certains cas, l'ensemble de ces problématiques peut se trouver très loin dans la liste des préoccupations de la direction jusqu'à ce qu'un incident vienne secouer les esprits. L'analyse de risque sera alors une réelle protection pour le DPO dans ce genre de situation.

Il y a aujourd'hui différents protocoles de messagerie existant en fonction du but recherché.

Apparu dans le début des années 80, le protocole SMTP (Simple Message Transfer Protocol) est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. Il permet l'envoi des messages.

Le SMTP est généralement utilisé via le port 25 en clair et via le port 465 ou 587 avec une sécurisation de type SSL.

Le protocole POP (Post Office Protocol), lui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.

Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. Actuellement le POP3 est un standard. Il permet de configurer simplement des clients de messagerie type Outlook, ThunderBird ou Lotus Note.

Le POP est généralement utilisé via le port 110 en clair et via le port 995 avec une sécurisation de type SSL.

Internet Message Access Protocol (IMAP) est quant à lui un protocole qui permet de récupérer les courriers électroniques déposés sur des serveurs de messagerie. Son but est donc similaire à POP3, l'autre principal protocole de relève du courrier.

Mais contrairement à ce dernier, il a été conçu afin que l'utilisateur puisse laisser ses mails sur le serveur. Cette fonctionnalité permet de les consulter à partir de différents clients de messagerie ou webmail. Il permet également de créer des dossiers ou de manipuler les messages directement sur le serveur.

Le protocole IMAP est généralement utilisé via le port 143 en clair et via le port 993 avec une sécurisation de type SSL.

Il s'agit pour l'organisme de ne pas abandonner des basiques de sécurité afin d'arranger des utilisateurs ne souhaitant pas changer leurs mauvaises habitudes ou adopter de bonnes pratiques.

Un des exemples les plus courants est l'utilisation d'un compte mail pour plusieurs utilisateurs, tous configurés en POP afin que les messages restent non lus pour l'ensemble des destinataires même si l'un d'eux l'a consulté, il s'agit du pire choix que l'on puisse faire.

On peut cumuler les mauvaises décisions en utilisant un compte Gmail ou Yahoo hébergé à l'étranger. Avec ce type d'organisation aucune mesure corrective immédiate n'est possible.

Afin de garder un contrôle optimal sur les données sous la responsabilité des effectifs de l'organisme, il est recommandé d'utiliser le protocole IMAP avec un chiffrement SSL ou un système de messagerie type Exchange sans jamais activer le protocole POP. En effet, une fois activé le protocole POP est une réelle faille de sécurité, une porte ouverte à d'imprévisibles situations qui sont rarement au bénéfice de l'organisme.

Ce choix de sécurité peut être paradoxalement considéré comme intrusif dans la vie privée des effectifs de l'organisme, mais encore une fois il est préférable d'imposer un contrôle à un nombre restreint d'utilisateurs pour assurer la protection d'un grand nombre de clients

L'IMAP permet un contrôle total des informations qui transitent. Ce protocole permet de stocker l'ensemble des courriers électroniques sur le serveur, et donc d'interagir efficacement en cas de situation de crise.

Le protocole POP doit impérativement être désactivé, car même en cas de messagerie fonctionnant avec le protocole IMAP, tant que le POP est activé il peut permettre à un compte externe de charger l'information.

Il faut également s'assurer que l'expédition SMTP et les réceptions IMAP soient cryptées avec une connexion SSL pour éviter toutes les DPI potentielles (Deep Packet Inspection).

L'intérêt d'un tel choix d'infrastructure répond au premier principe de Privacy by Design

Il convient d'anticiper de potentielles atteintes à la vie privée. La mise en place de ce type de réglage au sein de l'infrastructure de messagerie offrira la possibilité à l'organisme de prendre des mesures correctives immédiates et appropriées en cas de situation de crise.

Cet exemple met en relief l'importance du rôle du DPO dans les prises de décisions stratégiques de l'entreprise.

Certaines de ces décisions auront une réelle incidence sur la protection du patrimoine informationnel de l'entreprise.

Qu'elles soient techniques, pédagogiques ou spécifiques à la communication, la synergie des mesures à mettre en œuvre est un facteur clé de succès.

3.2. Méthode de stockage proactive (Storage's method enhancing privacy)

Les bases de données représentent aujourd'hui des actifs stratégiques pour les organismes qu'ils soient publics ou privés. Elles jouent un rôle majeur dans la fonction commerciale. Un grand nombre d'informations liées aux clients y sont stockées. On peut aussi y retrouver les informations inhérentes aux différents produits ou services. Elles représentent une véritable valeur économique au sein du patrimoine des entreprises et sont une composante clé de leur compétitivité. Comme tout objet de valeur, ce patrimoine informationnel suscite des convoitises.

Comme nous l'avons souligné précédemment, la pire situation à laquelle une plateforme numérique peut être confrontée mais qui pourtant est un grand basique du piratage s'appelle le "dump", c'est-à-dire l'extraction complète de la base de données de l'entreprise. Ce type d'attaque peut être effectué par des entités externes à l'organisme et notamment par des entreprises concurrentes. Ces attaques sont le plus souvent réalisées par des acteurs internes à l'entreprise qui se rendent responsables de fuites vers l'extérieur ou quittent l'entreprise en emportant avec elles les données[42].

Afin de lutter contre ces comportements, il est fondamental de prévenir toutes dérives potentielles en créant les conditions d'une protection adéquate de ces actifs immatériels. Le système de chiffrement symétrique est un dispositif technique qui permet de limiter les conséquences collatérales d'un piratage.

Pour rappel les données les plus sensibles comme les coordonnées bancaires d'un client ont l'obligation d'être stockées via un chiffrement symétrique dans les bases de données.

Il conviendra donc de mettre en place une méthode que nous appellerons "Key Framework" dont nous sommes à l'origine. Cette méthode est une mesure technique que nous avons mise en place au fil du temps dans des développements dont nous avons eu la charge.
Afin de mettre en place cette méthode, nous cumulerons plusieurs principes déjà cités précédemment comme l'atomisation, le chiffrement symétrique avec la méthode AES et le hashage.

[42] Le dump : http://fr.wikipedia.org/wiki/Dump

La première étape consiste à développer deux fonctions au sein du système, une fonction de chiffrage symétrique en AES 256 et une seconde qui permettra à l'interface de déchiffrer les informations qu'elle seule sera apte à afficher en clair.

La seconde étape sera la génération de la clé. Ce chiffrement reposera sur une clé symétrique. Nous recommandons de hasher un mot secret afin de la générer.
Pour optimiser la protection, les plus prévoyants pourront générer une clé alternative qui devra être utilisée par les deux fonctions si et seulement si les conditions liées à l'identification de l'environnement système ne sont pas vérifiées.

Une fois développées et testées ces deux fonctions ainsi que la clé devront être isolées dans une librairie dédiée. Ensuite, il faudra encoder cette librairie ainsi que le connecteur de base de données. Pour un développement en langage PHP nous recommandons des solutions telles que "ioncube[43]" pour l'encodage des fichiers.

Comme son nom l'indique, l'objectif de cette méthode est d'utiliser l'interface de la plateforme numérique comme clé. Seule l'interface permettra aux utilisateurs habilités d'afficher en clair les données sensibles chiffrées dans la base de données.

En cas de vol de la base de données, l'utilisation du principe d'atomisation en isolant la clé de la base de données rendra toutes exploitations malveillantes des données impossibles.

L'encodage de la librairie contenant la clé et les fonctions permettra à l'architecte du système d'information d'être le seul détenteur de la librairie originale encore en clair et d'offrir la possibilité aux développeurs d'utiliser ces fonctions sans en connaître les mécanismes ni la clé. Ce dispositif est une seconde utilisation du principe d'atomisation

L'utilisation de la clé alternative permettra d'éviter l'apparition de bug si l'impensable venait à arriver. En effet, si la plateforme et la base de données étaient volées toutes les deux, le fait de ne pas pouvoir identifier le serveur sur lequel la plateforme est habituellement hébergée activera l'utilisation de la clé alternative excluant tout bug possible qui pourrait aider des développeurs à comprendre certains mécanismes sans pour autant déchiffrer correctement les données protégées.

Nous recommandons également d'intégrer un système d'envoi de mail d'alerte contenant l'adresse du serveur sur lequel elle est hébergée à l'attention de l'architecte si la plateforme détecte qu'elle n'est pas hébergée sur l'adresse IP publique prévue. Ce système pourra donner l'alerte en cas d'intrusion non détectée.

Le choix des données à chiffrer devra être fait, en sachant que chaque champ chiffré ne pourra plus être utilisé dans les conditions des différentes requêtes effectuées par des administrateurs en base de données. Le code postal par exemple est une donnée qui est souvent utilisée pour filtrer une recherche client en fonction de différents secteurs géographiques. Il est donc conseillé de conserver en clair les champs utiles au bon fonctionnement des affaires.

[43] ioncube est un encodeur de fichiers PHP.

3.3. Gestionnaire Electronique de Documents & Privacy by ReDesign

Le concept de Privacy by ReDesign[44] est une extension du Privacy by Design. Une approche qui vise à appliquer les sept principes fondamentaux aux systèmes existants. Ce concept peut être plus difficile à mettre en œuvre étant donné que nous serons dans ce genre d'application souvent tributaires de contraintes d'intégrité imposées par le système.

Le Gestionnaire Électronique de Documents est aujourd'hui un élément-clé de la mémoire de l'organisme. Il a pour mission le stockage de fichiers comme les PDF souvent reliés à certains enregistrements de la base de données.

Au cours d'un développement d'une plateforme d'agrégation de comptes destinée à un réseau de courtiers en gestion de patrimoine, nous avons dû concevoir un module permettant d'enregistrer les jugements de tutelle ou de curatelle de clients ayant souscrit une assurance.

La méthode la plus simple pour lier le fichier PDF à un enregistrement client consiste à automatiser la syntaxe de nommage des fichiers en fonction de la date, du type de jugement et du numéro client. Cette méthode de nommage laissera la possibilité à un informaticien connaissant le système de trouver le fichier dont il a besoin en quelques secondes.

Afin d'exclure cette possibilité il conviendra d'utiliser le contrôle d'intégrité augmenté lors de la réalisation du nommage des fichiers. La syntaxe choisie précédemment devra être hashée, afin de ne donner aucune information sur le contenu d'un fichier via son nom. Il sera donc impossible de trouver rapidement un fichier pour les personnes habilitées à accéder à certains dossiers sensibles du serveur.

Le nom du fichier PDF contenant du jugement du 18 décembre 2008 de tutelle du client numéro 10535 sera : JT18122008C10535 (Jugement Tutelle 18 12 2008 Client 10535).
Le code JT18122008C10535 hashé en utilisant la méthode SHA1 correspond à l'empreinte suivante : 033a4eb289d10a5b00d378ac860e7fe2981f997d

L'empreinte sera le nom du fichier définitif. La plateforme pourra donc retrouver le fichier correspondant. Le code réappliquera ce raisonnement pour retomber sur la même empreinte.

Afin d'augmenter la complexité du raisonnement de nommage, on pourra appliquer en plus la technique du grain de sel en ajoutant un mot secret à la fin du code initial avant de le hasher. Le code sera alors JT18122008C10535motsecret

En sachant que pour protéger le mot secret utilisé comme grain de sel, il est vivement recommandé d'encoder ce raisonnement dans une librairie dédiée comme nous avons pu le voir précédemment.

[44] Privacy by ReDesign : Building a Better Legacy http://www.ipc.on.ca/images/Resources/PbRD-legacy.pdf

3.4. Un ange gardien numérique (Integrated Privacy Minder)

L'IPM un concept que nous avons créé la première fois pour l'intranet d'un réseau de courtier en assurances, il s'agit d'un ange gardien numérique intégré au sein même de la structure du système, il est présent dans l'ensemble de l'arborescence. C'est un module dont la plupart des autres seront dépendants. Il a vocation à répondre à l'ensemble des exigences des différents principes fondamentaux.

Le développement d'un IPM dans un système d'information permet de répondre au troisième principe «*Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques».*

Il permettra également d'anticiper et d'encadrer un grand nombre de scénarios critiques mis en avant dans l'étude d'impact que nous recommandons de réaliser au préalable. Anticiper ce type de scénario évitera de mettre en œuvre des parades a posteriori. Il s'agit de *«Prendre des mesures proactives et non réactives, des mesures préventives et non correctives*».

Pour répondre au second principe de «Privacy by default» en assurant «*la protection implicite des données»*, la solution consistera à mettre en place notre méthode «Key Framework» déjà définit précédemment afin d'assurer la protection des données les plus sensibles.

Pour mettre en application la notion «de cercle de confiance», on renseignera dans une table de la base de données l'ensemble des types de données utilisées, la ou les catégories auxquelles elles appartiennent, pour assurer que leur accessibilité soit restreinte aux différents profils d'utilisateurs autorisés en fonction des services.

L'ange gardien numérique a également la mission de protéger le patrimoine informationnel de l'organisme dans son ensemble. En effet afin de respecter le quatrième principe l'IPM ne doit pas se restreindre à la protection des données à caractère personnel.

Nous recommandons donc de :

- définir quelles sont les données dont l'extraction en interne est autorisée.
- limiter le nombre d'enregistrements contenus dans une extraction.
- limiter le nombre d'extractions possibles sur un laps de temps préalablement défini.

Concernant la modélisation du cycle de vie des données encadrée par le cinquième principe fondamental. Il conviendra de renseigner toutes les durées de conservation à respecter au sein de la table où nous aurons déjà listé toutes les données utilisées. L'IPM devra archiver automatiquement les données et attendre la validation d'un administrateur pour supprimer les données qu'il estime à présent sans pertinence.

Pour assurer un haut niveau de transparence attendu à travers le sixième principe, il convient d'effectuer la mise en place d'une traçabilité des utilisateurs appartenant aux effectifs de l'organisme. Ce système de traçabilité offrira à l'organisme un niveau de transparence adéquate. Il pourra en cas de contrôle indépendant présenter un historique de

toutes les actions effectuées par ses effectifs. Il faudra également rendre accessible à tous les durées de conservation appliquées par le système ainsi que les différents types de données et les catégories auxquelles elles appartiennent.

Pour répondre au septième principe «*Respecter la vie privée des utilisateurs*», il conviendra d'offrir un contrôle optimal aux utilisateurs ainsi qu'à toutes les personnes concernées, ils doivent être en mesure d'accéder à toutes les informations les concernant. Il s'agit de réaliser un système centré sur l'utilisateur comme expliqué infra.

4. INNOVATIONS ET PROSPECTIVES

Dans cette dernière partie, nous présenterons les SmartData, un concept considéré en Ontario comme un outil permettant de mettre en place un Privacy by Design de deuxième génération. Puis nous verrons une mise en œuvre possible du Privacy by Design à un niveau supérieur au service d'un article de loi du règlement européen. Nous finirons par vous présenter un principe qui pourrait peut-être un jour devenir le huitième.

4.1. SmartData & Ecosystème des Données Personnelles

Le SmartData est un concept qui a vocation d'assurer que le contrôle effectif sur les données personnelles soit uniquement et exclusivement offert aux personnes concernées, et non pas sous le contrôle d'un organisme.

La personne pourra assurer le contrôle des informations qui la concerne sans avoir à exercer une surveillance constante pour chaque demande d'information.

Le SmartData permet de faire en sorte que les données se protègent elles-mêmes. Ce dispositif sera donc intégré à toutes les opérations concernant ces données

Créé par le docteur George Tomko, ce concept est une nouvelle méthodologie pour protéger des données, dont l'objet est l'utilisation d'agents numériques artificiels.
Ces agents intelligents auront un rôle de Privacy Officer virtuel garant des accès à la donnée en fonction des habilitations autorisées par la personne concernée, un peu comme un proxy intégré à chaque fichier. Ils devront s'adapter à tout type de contexte transactionnel pour protéger les données en respectant les volontés paramétrées au sein de l'Ecosystème des Données Personnelles.

L'immense potentiel que présente l'Ecosystème des Données Personnelles tient dans le fait de confier exclusivement aux personnes concernées le contrôle de leurs informations.

D'après Ann CAVOUKIAN l'Ecosystème des Données Personnelles peut véritablement changer les règles du jeu. Il portera la protection de la vie privée au-delà des lois, des règlements et des pratiques exemplaires en permettant l'établissement d'une relation axée sur la protection des renseignements personnels entre les gens et les organismes[45].

[45] Rapport annuel 2012 du Commissariat à l'information et à la protection de la vie privée de l'Ontario http://www.ipc.on.ca/images/Resources/ar-2012-f.pdf

4.2. Protocole Normalisé d'Echange Sécurisé de Données à Caractère Personnel

Le Privacy by Design pourrait également être mis en œuvre à un niveau supérieur. En effet le premier principe se réfère à des mesures préventives et non pas réactives. Nous pourrions développer un "PET" au service d'un futur droit d'accès qui redonnerai le contrôle à l'utilisateur sur ses données.

Le projet de règlement européen publié le 25 Janvier 2012 prévoit la portabilité des données dans son article 18[46]. Il est intéressant de noter que le projet de rapport sur la proposition de règlement du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)[47] du 17 décembre 2012 de la commission des libertés civiles, de la justice et des affaires intérieures, et dont le rapporteur est Jan Philipp Albrecht, propose que cet article 18 sur le « Droit à la portabilité des données » soit intégré à l'article 15 sur le droit d'accès de la personne concernée.

Cette intégration a été confirmée suite aux modifications publiées dans la version consolidée[48] de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen menée par Jan Philipp Albrecht

Pouvons-nous alors espérer voir apparaître un nouveau format universel de fichier au service d'une nouvelle forme du droit d'accès qui respecterait un protocole normalisé d'échange sécurisé de données à caractère personnel avec l'arrivée de ce nouveau droit de portabilité des données ?

Ce format universel pourrait renforcer le contrôle de l'utilisateur : effectivement, si l'ensemble des plateformes respectaient le même protocole cela permettrait à l'utilisateur de rectifier, compléter, clarifier, mettre à jour ou encore effacer les informations le concernant avec le même type de fichier qu'il importerait ou exporterait lui-même sur sa plateforme hébergée par un tiers de confiance auxquelles les autres plateformes pourraient venir se connecter pour actualiser l'information en fonction des autorisations.

---

[46] Article 18 du projet de règlement : « *Droit à la portabilité des données :*
1. Lorsque des données à caractère personnel font l'objet d'un traitement automatisé dans un format structuré et couramment utilisé, la personne concernée a le droit d'obtenir auprès du responsable du traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré qui est couramment utilisé et qui permet la réutilisation de ces données par la personne concernée.
2. Lorsque la personne concernée a fourni les données à caractère personnel et que le traitement est fondé sur le consentement ou sur un contrat, elle a le droit de transmettre ces données à caractère personnel et toutes autres informations qu'elle a fournies et qui sont conservées par un système de traitement automatisé à un autre système dans un format électronique qui est couramment utilisé, sans que le responsable du traitement auquel les données à caractère personnel sont retirées n'y fasse obstacle.
3. La Commission peut préciser le format électronique visé au paragraphe 1, ainsi que les normes techniques, les modalités et les procédures pour la transmission de données à caractère personnel conformément au paragraphe 2. Ces actes d'exécution sont adoptés conformément à la procédure d'examen prévue à l'article 87, paragraphe 2. »

[47] (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

[48] La version consolidée[48] de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen menée par Jan Philipp Albrecht
http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

Ce format devrait être réalisé dans les règles de l'art. Il faudrait prendre en compte l'ensemble des principes de privacy by design, afin d'exclure toutes possibilités d'éventuelles dérives «Privacide» qui pourraient être provoquées par une utilisation malveillante du datamining.

Il conviendra donc de s'assurer que le contrôle effectif sur les données personnelles soit uniquement et exclusivement offert à la personne concernée.

En octobre 2013, l'organisation WM ADVANCED[49], a ouvert «le Projet 18» dont nous avons la charge, afin d'anticiper les éventuelles problématiques d'un futur développement.

L'objectif est de rédiger un cahier des charges afin de définir un ensemble d'exigences et d'effectuer une étude de faisabilité. Ce travail devra permettre d'établir des recommandations pour une mise en œuvre d'un tel protocole en adéquation avec les sept principes.

4.3. Privacy by Information

Dans le cadre de nos fonctions au sein de l'organisation WM ADVANCED, nous travaillons également sur une notion qui pourrait peut-être un jour devenir un huitième principe : «Privacy by Information».

Ce principe repose sur l'idée suivante :

Si le fait d'informer l'utilisateur à l'intérieur d'un système devenait un jour, une obligation juridique à respecter pour chaque action exécutée pouvant potentiellement avoir ou provoquer des conséquences sur les données à caractère personnel, cela imposerait à tous les informaticiens de connaître la loi informatique et libertés afin de pouvoir informer les utilisateurs qui utilisent leur logiciel ou naviguent sur leur site internet. Ce principe devra être mis en œuvre via des fenêtres de validation d'action qui expliqueraient les conséquences juridiques que peut entraîner telle ou telle action.

À la fois destiné aux concepteurs et aux utilisateurs, ce principe pourrait devenir une arme absolue d'éducation au numérique.

Une mise en œuvre généralisée de ce principe pourrait augmenter le niveau de culture informatique et libertés de l'ensemble des citoyens encore trop peu à être conscient des risques qu'ils encourent en tant qu'utilisateur et des conséquences que certaines de leurs actions peuvent provoquer.

[49] WM ADVANCED est une organisation qui travaille sur plusieurs projets d'innovation prospectives liés au Privacy by Design.

CONCLUSION

Notre avenir dépendra de la manière dont il sera codé. Le code a vocation d'intégrer l'ensemble de nos valeurs fondamentales, il est censé garantir nos libertés et protéger nos vies privées.

Nous, informaticiens, acteurs du numérique, choisissons tous les jours comment le code va se comporter. Nous l'écrivons. Nous sommes responsables du futur visage du monde numérique, nous devons prendre position pour concevoir un univers numérique respectueux des droits et des libertés. Nous devons coder pour protéger notre avenir.

Dès 1999 on pouvait déjà trouver ce type de message destiné à mettre au premier plan l'importance des algorithmes pour notre avenir dans l'article "Code is Law - On Liberty in Cyberspace" de Lawrence Lessig[50].

Le Privacy by Design a vocation d'encadrer la rédaction de ces codes qui seront par la suite considérés comme loi.

Le concept de Privacy by Design est la clé, il est bien plus qu'un article de loi ou de règlement, bien plus qu'une nouvelle norme reconnue à l'échelle mondiale.

Le concept de Privacy by Design est un ensemble de principes et de pratiques qui régissent les rapports entre les hommes et l'information.

Il s'agit d'un paradigme, une manière d'appréhender les choses, une vision cohérente du système qui repose sur une base définie, une matrice disciplinaire, un modèle théorique.

C'est une forme de rail de la conception dont les lois sont destinées aux concepteurs pour exprimer la façon dont un système d'informations ab initio doit être conçu et pensé dans ses grandes lignes afin d'assurer la conformité informatique et libertés.

"Article 1 de la loi informatique et libertés

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."

[50] Le code fait loi - De la liberté dans le cyberespace
http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig

Code is Law - On Liberty in Cyberspace http://harvardmagazine.com/2000/01/code-is-law-html

BIBLIOGRAPHIE

Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

Madrid, le 2 novembre 2009 «Respect de la vie privée dès la conception (Privacy by Design): le séminaire définitif» - «Privacy by Design : Tenir les promesses»
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-11-02_Madrid_privacybydesign_FR.pdf

Privacy-Enhancing Technologies: The Path to Anonymity
http://www.ipc.on.ca/images/Resources/anoni-v2.pdf

Loi Informatiques et libertés de 1978 modifiée en 2004
http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

Le 10 décembre 1948, les 58 États Membres qui constituaient alors l'Assemblée générale ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot (résolution 217 A (III)).
http://www.un.org/fr/documents/udhr/

Les sept principes fondamentaux
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

Les sept principes fondamentaux en français
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-f.pdf

Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices
http://www.privacybydesign.ca/index.php/paper/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/

Recommandation du parlement européen à l'attention du Conseil des ministres sur le renforcement de la sécurité et des libertés fondamentales sur Internet publiée le 26 mars 2009
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:117E:0206:0213:FR:PDF

Newsletter du CEPD
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_24_FR.pdf

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
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

DIRECTIVE 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:fr:PDF

Le Privacy by Design confronte à la disparition des piliers du Traité de Lisbonne publié par Anne CAMILLERI
http://www.ceric-aix.univ-cezanne.fr/fileadmin/CERIC/Documents/manifestations_scientifiques/Atelier_Privacy_by_design/camilleri_privacy_by_design__2_.pdf

Rapport du groupe «Droit à l'oubli[1]» de Cyberlex publié le 25 mai 2010
http://www.cyberlex.org/page-accueil/cyberlex-remet-son-rapport-droit-a-loubli.html

Rapport de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique du 22 juin 2011
http://www.assemblee-nationale.fr/13/rap-info/i3560.asp

Résolution historique lors de la conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu à Jérusalem. http://www.justice.gov.il/NR/rdonlyres/3FB67FDB-92DF-4DA0-9146-371DC1992F25/26502/ResolutiononPrivacybyDesign.pdf

La Federal Trade Commission (FTC) est une agence indépendante du gouvernement des États-Unis, créée en 1914 par le Federal Trade Commission Act. Sa mission principale est l'application du droit de la consommation et le contrôle des pratiques commerciales anticoncurrentielle tels que les monopoles déloyaux. La création de la FTC fut l'une des principales actions du président Woodrow Wilson contre les trusts. http://fr.wikipedia.org/wiki/Federal_Trade_Commission

Obama ne soutient pas le concept « privacy by design » Par Brian Beary à Washington le jeudi 22 mars 2012
http://www.europolitique.info/obama-ne-soutient-pas-le-concept-privacy-by-design-art329724-9.html

Présentation de la FTC : Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments
http://www.ftc.gov/os/2013/03/130306mobilereport.pdf

Federal Trade Commission recommends a Privacy by Design approach for mobile payment services
http://www.privacybydesign.ca/index.php/federal-trade-commission-recommends-a-privacy-by-design-approach-for-mobile-payment-services/

FTC Chief : Privacy Principles Should Govern 'Internet of Things' from Privacy & Data Security Law Resource Center
http://www.bna.com/ftc-chief-privacy-n17179880336/

Edward Joseph Snowden : http://fr.wikipedia.org/wiki/Edward_Snowden

Comment les révélations d'Edward Snowden ont touché le monde entier, un article de Pauline Hofmann, publié le 20/08/2013
http://www.francetvinfo.fr/monde/espionnage-d-internet/comment-les-revelations-d-edward-snowden-ont-touche-le-monde-entier_393730.html

La version consolidée[1] de la proposition du règlement européen le 22 octobre 2013 après le vote de la commission « Libertés civiles » (LIBE) du Parlement européen menée par Jan Philipp Albrecht
http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

COMMENT REALISER UNE EVALUATION D'IMPACT SUR LA VIE PRIVEE (EIVP) POUR LES DISPOSITIFS RFID ?
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Methodologie-etude_impact_RFID.pdf

Encryption by Default and Circles of Trust : Strategies to Secure Personal Information in High-Availability Environments http://www.privacybydesign.ca/content/uploads/2012/12/pbd-circlesoftrust.pdf

Operationalizing Privacy by Design http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf

GUIDE "Gestion des risques vie privée" Méthodes des mesures publié par la CNIL en 2012.
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf

Chiffrement par décalage : http://fr.wikipedia.org/wiki/Chiffrement_par_décalage

Loi pour la confiance dans l'économie numérique
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id

Fiche pratique : Un site marchand peut-il conserver mes données bancaires ? publié par la CNIL le 21 juin 2011
http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-site-marchand-peut-il-conserver-mes-donnees-bancaires/

Informatique légale : http://fr.wikipedia.org/wiki/Informatique_légale

Secret réparti : http://fr.wikipedia.org/wiki/Secret_réparti

Le dump : http://fr.wikipedia.org/wiki/Dump

Privacy by ReDesign : Building a Better Legacy http://www.ipc.on.ca/images/Resources/PbRD-legacy.pdf

Rapport annuel 2012 du Commissariat à l'information et à la protection de la vie privée de l'Ontario
http://www.ipc.on.ca/images/Resources/ar-2012-f.pdf

Le code fait loi - De la liberté dans le cyberespace
http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig

Code is Law - On Liberty in Cyberspace http://harvardmagazine.com/2000/01/code-is-law-html

ANNEXES

1. Article 23 publié dans la proposition de règlement européen du 25.01.2012

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals
with regard to the processing of personal data and on
the free movement of such data (General Data Protection Regulation)

Article 23
Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to a dopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

2. Article 23 publié dans la version consolidée après le vote LIBE du 22.10.2013

INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE
PROVIDED BY THE RAPPORTEUR
22 October 2013
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Article 23
Data protection by design and by default

1. Having regard to the state of the art, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, if any, shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular with regard to the principles laid out in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.

1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to the Directive of the European Parliament and of the Council on public procurement as well as according to the Directive of the European Parliament and of the Council on procurement by entities operating in the water, energy, transport and postal services sector (Utilities Directive).

2. The controller shall ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.

3. (deleted)

4. (deleted)

3. Article 5 publié dans la version consolidée après le vote LIBE du 22.10.2013

INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE
PROVIDED BY THE RAPPORTEUR
22 October 2013
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Article 5
Principles relating to personal data processing

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation);

(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data (data minimisation);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

(e) kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research or for archive purposes in accordance with the rules and conditions of Articles 83 and 83a and if a periodic review is carried out to assess the necessity to continue the storage, and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation);

(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);

(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity);

(f) processed under the responsibility and liability of the controller, who shall ensure and be able to demonstrate the compliance with the provisions of this Regulation (accountability).

4. Article 33 publié dans la version consolidée après le vote LIBE du 22.10.2013

INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE
PROVIDED BY THE RAPPORTEUR
22 October 2013
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Article 33
Data protection impact assessment

1. Where required pursuant to point c of Article 32a(3) the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data. A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.

2. (deleted, content moved to Article 32a(2)))

3. The assessment shall have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall contain at least

(a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller,

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation,

(d) a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed,

(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;

(f) a general indication of the time limits for erasure of the different categories of data;

(h) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;

(i) a list of the recipients or categories of recipients of the personal data;

(j) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(k) an assessment of the context of the data processing.

3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.

3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies.

The controller and the processor and, if any, the controller's representative, shall make the assessment available, on request, to the supervisory authority.

INDEX

CONTACT

email: alessandro@fiorentino-consulting.com
www.fiorentino-consulting.com

FIORENTINO Consulting
Protecting Privacy and Civil Liberties in the Digital Age