L'implémentation à la source et de haute qualité: le phénomène " by design by default "

Sarah Markiewicz

L'implémentation à la source et de haute qualité : le phénomène "by design by default"

S. Markiewicz, *doctorante en droit des technologies de l'information, LIDMS – AMU & CRDP - UdeM*

***Résumé* — Le but de cette contribution est de faire une lecture croisée des deux tendances-phares : le « *by design* » et le « *by default* ». Si la partie émergée de l'iceberg de ces deux tendances-phares touche le droit de la protection des données à caractère personnel avec le « *privacy by design* » et le « *privacy by default* », le réchauffement climatique permet de laisser entrevoir d'autres applications : le « *security by design* » et le « *security by default* ». L'enjeu de cette contribution est de savoir si les deux concepts sont compatibles voire applicables cumulativement, dans chacun de ces domaines respectifs et si cette duplication des concepts de « *by design* » et « *by default* » permet, à présent, d'identifier les objectifs poursuivis par chacun voire ensemble.**

Index des Termes* — *droit de la protection des données à caractère personnel, legal tech design, privacy by default, privacy by design, privacy enhancing technologies, security by default, security by design

I. INTRODUCTION

Ces deux courants que sont le « *by design* » et « *by default* » semblent vouloir réconcilier le droit avec l'informatique, la théorie avec la réalisation pratique, les avancées technologiques proactives et avant-gardistes avec les évolutions législatives, dont le processus est long, constituant souvent une réponse *a posteriori*. La question qui se pose est de savoir s'ils peuvent aussi dialoguer entre eux et s'enrichir mutuellement.

II. LE POINT DE DÉPART DU PHÉNOMÈNE : LE CONCEPT DE « PRIVACY »

A. Là où tout a commencé : le concept de "privacy by design"

Cette tendance « *by design* » est née outre-Atlantique au cours des années 1990 avec le concept de « *privacy by design*[1] » . On cite souvent la province canadienne de l'Ontario comme son berceau[2] et Madame Ann Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de 1997 à 2014 comme son porte-parole[3]. Il s'articule autour de sept principes fondamentaux : des mesures proactives ou préventives, une protection implicite et automatique, une intégration de la vie privée dans la conception des systèmes et au cœur des pratiques, une protection intégrale, une sécurité de bout en bout durant toute la conservation des données, une garantie de visibilité et transparence et le respect de la vie privée des utilisateurs[4]. Ce concept a pu traverser l'Atlantique grâce à sa consécration dans le Règlement européen 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 du 27/04/2016 dit « Règlement Général de Protection des Données » (RGPD) dont la traduction en français, moins populaire que sa version anglaise, est donc « protection des données dès la conception[5] ».

A cet égard, l'article 25 alinéa 1 du RGPD définit ce concept comme « *[la mise] en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées […] destinées à mettre en œuvre les principes relatifs à la protection des données […] de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent*

08/05/2017

S.Markiewicz, Laboratoire Interdisciplinaire en Droit des Médias et des Mutations Sociales (LID2MS), Université d'Aix-Marseille, Aix-en-Provence, P.A.CA., 13090, FRANCE; Centre de Recherche en Droit Public (CRDP), Université de Montréal, Montréal, QC, CANADA (e-mail: sarah.markiewicz@etu.univ-amu.fr).

[1] M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 476, oct. 2016 ; C. Zolynski, « La *Privacy by Design* appliqué aux Objets Connectés: vers une régulation efficiente du risqué informationnel ». *Dalloz IP/IT*, vol. 2016, n°9, p. 404, sept. 2016.

[2] Ibid., Commission Nationale pour la Protection des Données du Grand-Duché du Luxembourg (2015, mai). Le Privacy by Design: de quoi s'agit-il?. Luxembourg, Luxembourg. [en ligne]. Disponible: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_-de-quoi-s_agit-il_/index.html.

[3] Ibid. ; M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en oeuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 476, oct. 2016 ; C. Zolynski, « La *Privacy by Design* appliqué aux Objets Connectés: vers une régulation efficiente du risqué informationnel ». *Dalloz IP/IT*, vol. 2016, n°9, p. 404, sept. 2016.

[4] Commission Nationale pour la Protection des Données du Grand-Duché du Luxembourg (2015, mai). Le Privacy by Design: de quoi s'agit-il?. Luxembourg, Luxembourg. [en ligne]. Disponible: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_-de-quoi-s_agit-il_/index.html.

[5] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, 2016/679, 27 avril 2016, article 25 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679 ; M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 476, oct. 2016.

règlement[6] ». A l'instar de la notion-clé de consentement éclairé et informé préalable consacrée par le considérant 42 et l'article 7 du RGPD, l'emphase est mise sur son insertion dans la frise chronologique en amont de toute collecte ou traitement de données à caractère personnel, au moment de la détermination des moyens du traitement voire, au plus tard, au moment de sa réalisation[7]. D'un point de vue purement technique au sens informatique, il s'agit non pas de tenter de mettre en conformité des solutions ou systèmes techniques avec le droit de la protection des données à caractère personnel, notamment en cas d'évolution législative ou réglementaire, comme c'est bien souvent le cas mais d'encoder techniquement parlant les principes de droit de la protection des données à caractère personnel et ce dès les premières phases de conception d'un projet ou d'une solution informatique[8]. A titre d'illustration, l'anonymisation des personnes physiques citées dans les décisions de justice qui, à l'heure actuelle, est une opération *a posteriori* pourrait être prévue techniquement dès le début avec une exécution ultérieure à un instant précis.

L'enjeu repose surtout sur la capacité à traduire ces exigences théoriques juridiques en mesures techniques concrètes. Malgré tout, le RGPD donne des pistes pour implémenter ces critères juridiques et les convertir en mécanismes techniques de protection des données à caractère personnel : la minimisation des données et la pseudonymisation des données, comme le précisent le considérant 78 et l'article 25 alinéa 1 du RGPD[9]. La minimisation des données se trouve être, en réalité, un des piliers du cercle vertueux de la protection des données à caractère personnel prescrite par l'article 5 alinéa 1 point c) du RGPD comme « *[limité] à ce qui est nécessaire au regard des finalités pour lesquelles [les données à caractère personnel] sont traitées*[10] ». Quant à la pseudonymisation, il s'agit d'un « *traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable*[11] ». Elle est bel et bien vue comme une mesure de sécurité pour assurer la protection des données à caractère personnel, comme en témoignent l'article 6 alinéa 4 point e) et l'article 32 baptisé « Sécurité du traitement » alinéa 1 point a) du RGPD[12]. Les cas typiques et largement répandus et connus de pseudonymisation sont les célébrités et autres starlettes voire les personnes témoignant dans des articles de presse dont le nom est volontairement modifié (et indiqué par un astérisque au bas de l'article) pour préserver l'anonymat de cette personne. Ce procédé implique de protéger la table de concordance qui permettrait de réidentifier les personnes visées par les données pseudonymisées, le processus est donc réversible. A cet égard, il peut paraître moins absolu et jusqu'au-boutiste que celui d'anonymisation qui, lui, repose sur un procédé irréversible ne s'appuyant sur aucune table de concordance. D'un côté, il est possible de réidentifier la personne concernée moyennant une opération de correspondance alors que de l'autre côté, les données rendues anonymes ne permettent plus de réidentifier la personne concernée, selon le considérant 26 du RGPD[13].

B. To Be Continued : le concept frère jumeau de "privacy by default"

Cette expression « par défaut » nous vient du monde de l'informatique où elle est employée pour désigner « *une donnée ou une valeur attribuée automatiquement par le programme en l'absence d'une indication explicite de la part de l'utilisateur et qui représente habituellement le choix ou le réglage le plus probable, compte tenu du contexte*[14] ».

Le Règlement Général de Protection des Données a aussi apporté dans sa hotte le concept de « *privacy by default* », dont la traduction française est « protection des données par défaut ». L'article 25 alinéa 2 l'évoque en ces termes : « *[la garantie, par défaut, que] seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées*[15] ». Il vise donc un paramétrage technique, de prime abord, qui soit un respect scrupuleux de trois des principes moteurs du cercle vertueux de collecte et de traitement des données à caractère personnel prévu à l'article 5 susmentionné dudit Règlement[16]. Il s'agit, en fait, d'une triple interprétation du principe de proportionnalité[17], eu égard la typologie des données à caractère personnel réclamées (le principe de spécification des finalités de la collecte ou du traitement), leur quantité (le principe de minimisation des données) et leur conservation limitée dans le temps (le principe de limitation de la

[6] Ibid., article 25 alinéa 1.
[7] Ibid., considérant 42 et article 7.
[8] M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 477, oct. 2016.
[9] Ibid., *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016, considérant 78 et article 25 alinéa 1 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.
[10] Ibid., article 5 alinéa 1. point c).
[11] Ibid., article 4 point 5).
[12] Ibid., article 6 alinéa 4 point e) et article 32.
[13] Ibid., considérant 26.
[14] Dictionnaire de l'informatique et d'internet : http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20040107183752.
[15] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016, article 25 alinéa 2 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.
[16] Ibid., article 5.
[17] C. Zolynski, « La *privacy by design* appliqué aux Objets Connectés: vers une régulation efficiente du risqué informationnel ». *Dalloz IP/IT*, vol. 2016, n°9, p. 405, sept. 2016.

conservation[18]) : « *Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité*[19] ». Comme précédemment décrit, le principe de minimisation des données se préoccupe de limiter la collecte et le traitement des données à caractère personnel au strict nécessaire : exit le postulat du « *Vaut mieux trop que pas assez* » au profit du « *Juste ce qu'il faut* ». Pour ce qui est du principe de spécification des finalités de la collecte et du traitement, il s'attarde plus sur la typologie des données à caractère personnel qui doivent être « *collectées pour des finalités déterminées, explicites et légitimes* », selon l'article 5 alinéa 1 point b)[20]. En d'autres termes, une concordance doit exister entre les objectifs poursuivis et les données réclamées en vue d'une collecte ou d'un traitement. On peut imaginer cohérent de demander un identifiant et mot de passe pour s'authentifier et se connecter à une session informatique mais non si pour ce faire, il était requis de renseigner son dernier bilan sanguin, qui relève, d'ailleurs du champ des données médicales mais aussi celles dites « sensibles ». Pour finir le principe de limitation de la conservation se donne pour objectif de lutter contre toute réutilisation incompatible avec les finalités de la collecte ou du traitement prévues, comme on le retrouve dans la seconde portion du principe de spécification des finalités : « *et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités*[21] » et souligne que la conservation doit se borner à « *une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* », d'après l'article 5 alinéa 1 point e[22]). Par conséquent, l'implémentation du concept de « *privacy by default* » peut se résumer à encoder le principe conducteur de proportionnalité dans trois dimensions : quantitative, qualitative et temporelle.

On peut également ajouter que ce concept rejoint un des points visés par la définition du concept de « *privacy by design* » proposée par Ann Cavoukian, à savoir celui de protection intégrale qui doit s'opérer *de facto* sans démarche préalable de la personne concernée[23]. Cela consisterait pour cette dernière à approuver ce pré-paramétrage plutôt bienveillant à son égard ou à donner son consentement en vue de quelques aménagements témoignant d'un lâcher-prise par rapport au respect scrupuleux des principes du cercle vertueux de la collecte ou du traitement des données à caractère personnel quant aux siennes. Cela rappelle les débats entre les logiques « *opt-in* » et « *opt-out* » à propos du consentement crystallisés dans le considérant 42 du RGDP[24]. La première se matérialise par le fait qu'on attend une démarche proactive de l'internaute qui coche, par exemple, une case ; ce qui est la théorie prônée en Europe, à laquelle on oppose la seconde qui requiert une démarche de réaction contestataire où l'internaute doit décocher une case qui a été précochée ; ce qui prévaut plutôt aux Etats-Unis. En l'occurrence, on peut y voir l'application du concept d' « *opt-out* » car la démarche est de fait et antérieure à toute démarche opposée de la personne concernée. Or, dans ce cas de figure, la démarche est bienveillante : proposer les options les plus protectrices quant aux données à caractère personnel de la personne concernée et à son libre arbitre et non malveillante telle que dans le contexte du droit du commerce électronique où les mesures de protection relatives au droit de la protection des données à caractère personnel sont suggérées ou installées a minima incitant la personne concernée à prendre la main si elle souhaite les renforcer pour que les principes susmentionnés s'appliquent bien à la collecte ou au traitement de ses données à caractère personnel.

Or, il faut souligner que dans les faits, les concepts de « *privacy by design* » et « *privacy by default* » ne sont pas des frères ennemis mais plutôt les deux faces d'une même pièce. D'ailleurs, le principe de minimisation des données est présent au sein de ces deux concepts. Ils ne sont pas incompatibles et peuvent être cumulés car le second est inclus dans le premier. De plus, la somme des deux concepts donnerait naissance à celui de « *privacy by design by default* » qui sous-entendrait un encodage des principes du droit de la protection des données à caractère personnel dès le début de la mise en place d'un système informatique et ce, d'office, par défaut. En outre, la combinaison des principes de la protection des données à caractère personnel de chaque concept correspond plus ou moins à ceux principaux prescrits par l'article 5 du RGPD retraçant les étapes du cercle vertueux de la collecte et du traitement des données à caractère personnel.

III. LE PASSAGE OBLIGÉ : LE CONCEPT DE « SECURITY »

A présent, nous rencontrons un peu partout des clones ou petit(e)s frères/sœurs des concepts de « *privacy by design* » et « *privacy by default* » qui commencent à voir le jour comme les concepts de « *(computer) security by design* » et « *(computer) security by default* » pour la sphère de la sécurité informatique.

A. Le clone informatique né après : le "security by design"

L'adjonction du suffixe « *by design* », qui se traduit en

[18] M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en œuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 477, oct. 2016.

[19] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016, article 25 alinéa 2 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

[20] Ibid., article 5 alinéa 1 point b).

[21] Ibid.

[22] Ibid., article 5 alinéa 1 point e).

[23] Commission Nationale pour la Protection des Données du Grand-Duché du Luxembourg (2015, mai). Le Privacy by Design: de quoi s'agit-il?. Luxembourg, Luxembourg. [en ligne]. Disponible: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_-de-quoi-s_agit-il_/index.html.

[24] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016, considérant 42 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

français par « dès la conception » implique là aussi de construire une architecture informatique sécurisée dès le départ, faisant même partie de l'A.D.N. même de cette infrastructure, et non comme un revêtement qui s'appliquerait par la suite[25]. A l'instar des sept piliers fondateurs du concept de « *privacy by design* », le concept de « *security by design* » est pourvu de dix principes qui sont les suivants : minimiser la zone d'attaque, établir des mesures de sécurité par défaut, le principe de séparation des privilèges (plus connu sous le libellé anglais de « *Principle of Least privilege* »), le principe de défense en profondeur (plus connu sous le libellé anglais de « *Principle of Defense-in-depth* »), sécuriser même les procédures d'échec, ne pas faire une confiance aveugle en la sécurité informatique des services externes, le principe de séparation des tâches (plus connu sous le libellé anglais de « *Principle of Segregation of Duties* »), éviter l'implémentation d'une sécurité informatique basé sur la non-divulgation, conserver la sécurité informatique simple/ne pas la complexifier inutilement et réparer correctement les conséquences informatiques d'une action[26]. Ce corpus de règles se retrouvent à la section « principes de sécurité (informatique)[27] » d'un guide pour les développeurs dont la version 1.0 date de fin juin 2002 et celle 2.0 de juillet 2005 (la version 3 est encore d'élaboration depuis 2007). La rédaction de ce manuel d'utilisation émerge d'un projet baptisé « *Open Web Application Security Project* » (OWASP).

Le critère de devoir minimiser la zone d'attaque attire l'attention sur le fait que chaque nouvelle fonctionnalité d'une application informatique induit un risque pour le bon fonctionnement de l'application dans son ensemble[28]. Il faut donc réduire le risque inhérent à l'ajout d'une nouvelle fonctionnalité par rapport à l'écosystème de l'application informatique[29]. Pour ce faire, il est suggéré de restreindre l'accès de cette nouvelle fonctionnalité, dans un premier lieu, au responsable ou à l'équipe informatique pour limiter l'impact[30]. Ensuite, le fait de vouloir établir des mesures de sécurité par défaut renvoie directement au concept de « *security by default* » qui sera étudié dans un second temps. Le principe de séparation des privilèges repose sur le fait de créer des profils d'utilisateurs avec des droits d'accès ou d'action différents. Ainsi, un employé lambda d'une entité devrait se voir attribuer un profil d'utilisateur et des droits lui permettant d'accomplir ses tâches professionnelles sans autres droits qui seraient, dès lors, superflus car ne concourant pas à cet objectif[31]. A l'inverse, un poste à haute responsabilité devrait se voir associer un profil d'utilisateurs avec des droits plus larges que le précédent. Dans tous les cas, la mission principale du responsable informatique étant de veiller au bon fonctionnement du système informatique, il aura bien souvent un rôle du type « administrateur » pour pouvoir gérer la sécurité informatique du système sans pouvoir inférer sur le contenu même du système informatique[32]. Pour ce qui est du principe de défense en profondeur, il pourrait se résumer à l'adage « *Plutôt deux fois qu'une*[33] ». En effet, il consiste à ne pas faire reposer sa stratégie de sécurité informatique sur une seule et unique mesure technique comme un pare-feu mais de dédoubler les mesures de protection informatique telles que les démultiplier tout au long d'un processus[34], les coupler : une demande d'authentification doublée d'un procédé de cryptage pour les données qui le requièrent[35]. Puis, le critère œuvrant pour sécuriser même les procédures d'échec[36] sous-entend deux choses. D'une part, ne pas baliser avec des mesures de sécurité les processus d'impossibilité de se déconnecter ou de déconnexion laisse entrevoir une porte d'entrée pour les failles de sécurité. D'autre part, le concept de « *security by design* », en plus d'être implémenté en amont, semble aussi jusqu'au-boutiste, tout comme le concept de « *privacy by design* » qui prévoit une protection intégrale et de bout en bout pour la collecte et le traitement des données à caractère personnel. Ce point se vérifie, d'ailleurs, avec l'exigence de ne pas faire une confiance aveugle en la sécurité prétendue des systèmes informatiques externes[37]. Il faudra donc vérifier la sécurité de toute donnée entrante ou toute connexion ou interface avec un système informatique externe et ne pas déduire une présomption de sécurité optimale ou adéquate de leur part[38]. En ce qui concerne le concept de séparation des tâches, il repose essentiellement sur une bonne gestion des droits d'accès par profil et un non-cumul des profils ou des droits afférents. En d'autres termes, l'utilisateur qui demande une autorisation ne doit pas être celui qui doit également statuer sur sa validation ou son rejet. Les principes de séparation des privilèges et des tâches sont intrinsèquement liés puisque là où l'un définit des profils d'utilisateurs, l'autre détermine les actions permises ou autorisées par le profil d'utilisateurs en question. Quant au conseil de ne pas bâtir son architecture de sécurité informatique sur la non-divulgation, il lève le voile sur le talon d'Achille de ceux qui prônent « *Pour vivre en sécurité, vivons cacher* », à savoir que la seule mesure de sécurité, le seul rempart de protection est le secret. Autrement dit, toute divulgation compromettrait grandement la sécurité technique de la solution informatique[39]. Le concept de « *security by design* » donne raison aux défenseurs des solutions informatiques « *open source* » qui promeuvent

[25] Wikipedia : https://en.wikipedia.org/wiki/Secure_by_design

[26] Wikipedia : https://www.owasp.org/index.php/Security_by_Design_Principles#Security_principles

[27] OWASP (2005, juillet). "A Guide To Building Secure Web Applications and Web Services V2.0", p. 34 [En ligne]. Disponible : https://sourceforge.net/projects/owasp/files/Guide/2.0.1/OWASPGuide2.0.1.pdf/.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid., p. 36.

[33] Ibid., p. 35.

[34] Ibid.

[35] Wikipedia : https://fr.wikipedia.org/wiki/D%C3%A9fense_en_profondeur ; https://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf

[36] OWASP (2005, juillet). "A Guide To Building Secure Web Applications and Web Services V2.0", p. 35 [En ligne]. Disponible : https://sourceforge.net/projects/owasp/files/Guide/2.0.1/OWASPGuide2.0.1.pdf/.

[37] Ibid.

[38] Ibid.

[39] Ibid., p. 36.

davantage le slogan « *Nous n'avons rien à cacher … nous restons sécurisés* » puisqu'une solution informatique doit offrir une sécurité technique, même si on peut avoir accès à son code source. A cet égard, on peut relever le bras de fer entre les concepteurs de systèmes ou logiciels propriétaires comme Microsoft qui prônent la non-divulgation du code source alors que d'autres comme Linux ou OpenOffice privilégient une totale transparence à ce sujet[40]. Pour finir, l'avant-dernier critère recommande de ne pas complexifier une architecture informatique par diverses mesures de sécurité quand une mesure technique simple et efficace peut parfaitement convenir[41]. On peut noter que ce prérequis entre directement en contradiction avec le principe de défense en profondeur qui veut que chaque échelon de l'architecture informatique soit techniquement sécurisé. Le dernier point de cette liste des principes de sécurité informatique prône une attitude réactive en cas de détection de failles de sécurité qui se penche sur les causes de celles-ci en vue de mener rapidement des tests pour proposer des mesures correctives adaptées[42].

Le concept de « *security by design* » met en avant donc une sécurité informatique à tous les échelons d'un système informatique et considère qu'une gestion centralisée et globale de la sécurité informatique est bien mais non suffisante, surtout si elle peut être meilleure en l'implémentant dans toutes les strates de l'architecture informatique du système. Il fait également appel à une nécessaire classification, typologie des données et des mesures de sécurité afin de proposer celle la plus adaptée, parmi celles possibles d'instaurer, à chaque échelon ou nœud de l'architecture informatique du système[43].

B. Le "security by default" : l'un des paramètres du clone informatique

L'étude du concept de « *security by design* » semble indiquer en filigrane qu'il comprend celui de « *security by default* » puisque ce dernier est l'un des dix principes de « *security design* ». Tout comme le concept de « *privacy by default* » où la barrière de protection des données à caractère personnel est placée volontairement très haut et c'est à la personne concernée, si elle le souhaite, de la rabaisser, le concept de « *security by default* » implique que les mesures de sécurité instaurées soient renforcées et non disproportionnées par rapport aux exigences que requièrent les actifs en question. La main revient à l'utilisateur qui, s'il le souhaite, peut revoir ces mesures techniques de sécurité informatique à la baisse[44]. A titre d'exemple, pour se connecter à une session informatique, on a tendance à vous redemander à chaque fois les mêmes informations (identifiant et mot de passe). Dans certains cas, notamment, la connexion à un compte de messagerie électronique, on peut vous laisser la liberté via une option à cocher d'enregistrer l'appareil qui a servi d'interface de connexion (smartphone, tablette, ordinateur portable, etc.) pour vous éviter la peine de ressaisir ces informations, à chaque fois. Cependant, comme prescrit, c'est l'utilisateur qui accepte, de son propre chef, de baisser le niveau de sécurité renforcé reposant sur la conception d'usage unique.

IV. L'EMERGENCE DU CONCEPT « BY DESIGN DY DEFAULT »

A. Les concepts de "… by design" et les concepts de " … by default"

Avant toute chose, il faut souligner que les concepts de « *by design* » et « *by default* » ont été formalisés, d'abord, par le droit et après, par l'informatique alors que bien souvent, la pratique et la technique supplantent les évolutions législatives. L'autre constat est que les concepts de « *privacy by design* » et « *security by design* » semblent être bien plus vastes que les concepts de « *privacy by default* » et « *security by default* » : les premiers incluant les seconds, respectivement dans leur domaine. Si la lecture de l'article 25 du RGPD semble vouloir distinguer les concepts de « *privacy by design* » et « *privacy by default* », force est de constater que le lot de principes découlant du concept de « *privacy by design* » élaboré par Ann Cavoukian incorpore, sans le nommer explicitement, le concept de « *privacy by default* ». Les travaux du projet OWASP aboutissent à la même conclusion en matière de sécurité informatique : le concept de « *security by default* » est une brique du concept de « *security by design* ».

Si le RGPD traduit « *by design* » par « dès la conception », le guide édité par le consortium OWASP rejoint cette traduction puisque le concept de « *security by design* » requiert que les logiciels soient, dès leur phase de développement, conçus comme sécurisés[45]. Comme le droit de la protection des données à caractère personnel et la sécurité informatique s'accordent sur l'objectif premier ou la définition globale de leurs concepts de « *privacy by design* » et « *security by design* », le recours à une liste de principes variant de sept à dix semblent aller bien au-delà de ce but commun. Par ailleurs, cette liste de prérequis, de part et d'autre, sèment le doute et semblent alourdir la charge de l'encodage technique de principes de droit de la protection des données à caractère personnel et d'une sécurité informatique optimale voire trop parfaite. Les précédents développements ont, certes, permis de concilier et hiérarchiser, d'un côté comme de l'autre, les principes de « *privacy by design* » et « *privacy by default* » ainsi que les principes de « *security by design* » et « *security by default* ». Cependant, une application cumulée de tous les principes des concepts de « *privacy by design* » et « *security by design* » semble peine perdue.

Une lecture croisée des sept principes du concept « *privacy by design* » tend à se résumer à une prise en compte scrupuleuse et d'office du droit de la protection des données à caractère personnel et donc à l'application de l'article 5 du RGPD en amont. Pour rappel le respect des principes fondamentaux du

[40] Ibid.
[41] Ibid.
[42] Ibid., p. 37.
[43] Wikipedia : https://www.owasp.org/index.php/Security_by_Design_Principles.
[44] OWASP (2005, juillet). "A Guide To Building Secure Web Applications and Web Services V2.0", p. 34 [En ligne]. Disponible : https://sourceforge.net/projects/owasp/files/Guide/2.0.1/OWASPGuide2.0.1.pdf/.
[45] Wikipedia : https://en.wikipedia.org/wiki/Secure_by_design.

cercle vertueux de la collecte ou du traitement des données à caractère personnel consiste à demander l'accord préalable de la personne concernée, ne collecter et traiter que les types de données nécessaires, en quantité non excessive et ne les garder que le temps requis pour mener à bien les opérations indiquées et ce, en toute sécurité. Son application concrète paraît matériellement faisable en s'appuyant sur des filtres techniques et des pré-paramétrages de traitement de données à caractère personnel de type anonymisation, pseudonymisation ou destruction prévues en amont. Comme certains auteurs le suggèrent, cela peut reposer également sur une participation active de la personne concernée, en vertu du droit à l'autodétermination informationnelle[46]. On peut imaginer, par exemple, que cette dernière choisit librement les données à caractère personnel nécessaires à la collecte ou au traitement en question, leur nombre, parmi celles que le tiers réclame par défaut et valide la durée de conservation, fixée a minima conformément au droit ou accepte volontairement de l'étendre. En revanche, rien n'est moins sûr avec les dix principes du concept de « *security by design* ».

Et pour cause, le concept de « *privacy by design* » s'appuie sur des mesures techniques de sécurité informatique pour assurer cet objectif, le concept de « *security by design* » en appliquant plus ou moins les mêmes lignes directrices en matière de sécurité informatique paraît plutôt conduire à une surenchère à ce propos. Ce dernier semble baliser le périmètre de sécurité informatique pour ne pas laisser de place à un problème informatique en « verrouillant » informatiquement parlant tous les nœuds ou points d'accès, de connexion. Ces principes de sécurité informatique visent davantage une sécurité informatique pure et parfaite alors que le risque zéro, même en informatique, n'existe pas mais ils tendent quand même au 99%. On peut recommander de prioriser ces principes et d'écarter ceux adoptant une approche jusqu'au-boutiste. Par exemple, le fait de vouloir minimiser la zone d'attaque, ne pas faire une confiance aveugle en la sécurité informatique de services externes ou encore le principe de défense en profondeur témoignent d'un vœu pieu de tout contrôler, même ce qui est imparable. D'ailleurs, démultiplier les mesures de sécurité entre en contradiction avec la réserve émise qui vise à ne pas complexifier inutilement la sécurité technique de l'infrastructure informatique. Toutefois, les principes de séparation des privilèges et des tâches concourent à une volonté raisonnée d'organisation de l'architecture informatique en interne, notamment pour pouvoir appliquer une mesure technique vraiment renforcée quand cela s'avère nécessaire et non selon l'adage « *Qui peut le plus, peut le moins* ».

Pour finir, les principes de *« privacy by default* » et « *security by default* » apportent une précision nécessaire aux options informatiques par défaut. Si pendant un temps, la signification de paramétrage par défaut voulait dire des paramètres répondant aux minima requis, ils inversent la tendance en exigeant que ces paramétrages par défaut doivent plutôt être élevés pour assurer une protection des données à caractère personnel ou une sécurité informatique accrue.

B. Les concepts de "privacy by design by default" et de "security by design by default"

Etant donné que les deux domaines dans lesquels les concepts de « *by design* » et « *by default* » se sont illustrés concomitamment sont le droit de la protection des données à caractère personnel et la sécurité informatique, ils constituaient les cas d'étude idéaux pour tester le cumul applicatif des deux concepts donnant celui de « *privacy by design by default* » et celui de « *security by design by default* ».

Dans le cadre du droit de la protection des données à caractère personnel, le cumul des concepts de « *privacy by design* » et « *privacy by default* » se traduit par une application quasiment à la lettre du cercle vertueux de la collecte ou du traitement des données à caractère personnel. Cela signifie qu'au moment de déterminer les finalités de la collecte ou du traitement et d'en informer la personne concernée qui doit délivrer son consentement et au plus tard, au moment de sa réalisation, le responsable du traitement doit prévoir des paramétrages techniques qui s'enclencheront dès le début de la phase de réalisation avec peut-être une exécution différée dans le temps. Ainsi, il plébiscitera des mesures techniques de préférence implémentées *de facto* pour cibler le strict minimum des données à caractère personnel requises. Pour aller plus loin, on peut imaginer telles les options à cocher dans un questionnaire dynamique, une information préalable de ce qui représente des données à caractère personnel absolument nécessaires à la collecte et au traitement de ces données parmi celles que la personne concernée peut et souhaite communiquer. Une mise en garde s'impose. Il ne s'agit des actuels astérisques rouges dans un formulaire dynamique qui empêchent de valider la page web car certaines informations semblent, de nos jours, davantage additionnelles qu'indispensables. Cela sous-entend un reparamétrage pour les responsables de traitement qui en ont la tâche plus aiguisée visant à réduire celles collectées et traitées pour l'heure à un jeu de données à caractère personnel fondamentales par rapport à l'opération en question. Quant à la durée de conservation des données à caractère personnel, une protection intégrale est requise jusqu'à l'expiration de la durée de conservation. Cette information entre dans le devoir d'information préalable du responsable du traitement à l'égard de la personne concernée, énoncé à l'article 14 alinéa 2 point a) du RGPD[47], qui est aussi un des principes du concept de « *privacy by design* » promu par Ann Cavoukian. Une

[46] L. Cluzel-Métayer, « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », AJDA, vol. 2017, n°6, p. 344, fév. 2017 ; M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en oeuvre ». *Dalloz IP/IT*, vol. 2016, n°10, p. 476, oct. 2016 ; C. Zolynski, « La *Privacy by Design* appliqué aux Objets Connectés: vers une régulation efficiente du risqué informationnel ». *Dalloz IP/IT*, vol. 2016, n°9, p. 405, sept. 2016.

[47] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016, article 14 alinéa 2 point a) [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679.

application renforcée de la protection des données à caractère personnel sous-entend une anonymisation ou pseudonymisation voire destruction dès la fin du traitement de données à caractère personnel. Le rôle crucial joué par la personne concernée qui est rappelé indirectement par le dernier principe de la définition canadienne du concept de « *privacy by design* » pourrait se traduire par un choix offert à la personne concernée entre l'une de ces trois options, dès expiration de la durée de conservation. La personne concernée pourrait même pouvoir avoir son mot à dire sur cette durée de conservation car c'est une chose de devoir l'en tenir informée mais une tout autre chose de devoir justifier la nécessité d'une telle durée. On peut ajouter que le principe d'exactitude des données qui doivent être mises à jour ou rectifiées en cas de besoin, inscrit à l'article 5 alinéa 1 point d) du RGPD[48], peut être rapproché plutôt des droits de la personne concernée. Pour finir, il faut rappeler que les options ou paramétrages proposés à la personne concernée en lien avec la gestion de ses données à caractère personnel doit être bienveillante à l'égard de cette dernière et non configurée pour profiter d'abord à l'entité pour qui travaille le responsable du traitement. Ces configurations par défaut doivent permettre de renforcer l'application et le respect de la protection des données à caractère personnel. On peut citer, en ce sens, les « *Privacy Enhancing Technologies* » (P.E.T.) qui comme leur nom l'indique, suggèrent un renforcement du respect de la vie privée et, par extension, du droit de la protection des données à caractère personnel grâce aux technologies. Elles se focalisaient davantage sur la préservation de l'anonymat et la pseudonymie en ligne en lien direct avec la notion de confidentialité en sécurité informatique. On peut espérer un développement de leur part pour implémenter le principe de proportionnalité en droit de la protection des données à caractère personnel dans ses trois dimensions : qualitative, quantitative et temporelle.

Dans le cas de figure de la sécurité informatique, le cumul des concepts de « *security by design* » et « *security by default* » devrait se limiter à une sécurité informatique renforcée implémentée au cœur même des phases de développement de l'architecture informatique d'un système ou d'un logiciel informatique. L'armada de mesures de sécurité mise en avant par le concept de « *security by design* » est bien trop lourde à mettre en place. On pourrait envisager une déclinaison « *soft* » de ce concept qui reposerait davantage sur une bonne organisation en interne via les principes de séparation des pouvoirs et des tâches et une mesure de sécurité la plus élevée possible en fonction des actifs concernés. Ce dernier point rejoint le principe de proportionnalité évoqué en droit de la protection des données à caractère personnel quant aux réponses techniques à fournir : des informations classées « secret défense » ou vitales pour une entité nécessiteront des mesures de sécurité bien plus renforcées que celles dévolues à la communication de contenus dans un intranet dont l'accès repose sur une authentification.

[48] Ibid., article 5 alinéa 1 point d).

V. Conclusion

En résumé, l'implémentation du concept de « *privacy by design by default* » se trouve facilité par une hiérarchisation de ses composants et un concept de « *privacy by design* » dont les exigences semblent raisonnables et en adéquation avec l'objectif poursuivi de protection des données à caractère personnel. Par contre, le concept de « *security by design by default* » en l'état pourrait être rebaptisé « hard security by design by default » auquel il serait préférable de substituer une version « *soft security by design by default* ». Les P.E.T. confirment les suppositions émises en introduction, à savoir que la technologie et le droit, en l'occurrence, de la protection des données à caractère personnel ; peuvent se réconcilier et travailler au même tempo : la première aidant le second. On peut espérer un développement dans la même veine qu'on pourrait nommer « *law enhancing technologies by design* » ou « *legal tech by design* » où la technologie encoderait le droit à la source pour renforcer son respect et son application. Cette attitude proactive en amont se révèle être le strict opposé des audits de conformité actuels réalisés sur des systèmes ou solutions informatiques en phase de finalisation de conception. On peut imaginer qu'il est plus aisé de « *Prévenir que guérir* » est donc d'anticiper techniquement parlant les exigences juridiques que d'apporter des correctifs techniques à un système ou une solution déjà élaboré(e).

Bibliographie:

[1] Commission Nationale pour la Protection des Données du Grand-Duché du Luxembourg (2015, mai). Le Privacy by Design: de quoi s'agit-il?. Luxembourg, Luxembourg. [en ligne]. Disponible: https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/Le-Privacy-by-Design_-de-quoi-s_agit-il_/index.html

[2] *Règlement (UE) 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données*), 2016/679, 27 avril 2016 [en ligne]. Disponible :http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

[3] L. Cluzel-Métayer , « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit », AJDA, vol. 2017, n°6, fév. 2017

[4] M. Dary et L. Benaissa, « P*rivacy by Design* : un principe de protection séduisant mais complexe à mettre en oeuvre ». *Dalloz IP/IT*, vol. 2016, n°10, oct. 2016

[5] C. Zolynski, « La *Privacy by Design* appliqué aux Objets Connectés: vers une régulation efficiente du risqué informationnel ». *Dalloz IP/IT*, vol. 2016, n°9, sept. 2016.

[6] Dictionnaire de l'informatique et d'internet : http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20040107183752

[7] site internet Wikipedia : https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal

[8] site internet OSDN : https://fr.osdn.net/

S. Markiewicz détient une Licence en droit, une Maîtrise en droit des affaires et un Master en droit de la banque et des opérations patrimoniales de l'Université d'Aix-Marseille ainsi qu'un Master complémentaire en Droit des Technologies de l'Information et de la Communication de l'Université de Namur (Belgique). Elle est doctorante en droit des technologies de l'information au Centre de Recherche en Droit Public (C.R.D.P.) de l'Université de Montréal (CANADA), sous la direction du Professeur Nicolas Vermeys, et au Laboratoire Interdisciplinaire en Droit des Médias et des Mutations Sociales (L.I.D.2.M.S.) de l'Université d'Aix-Marseille, sous la direction du Professeur Hervé Isar. Elle est également chargée de travaux dirigés à l'Université d'Aix-Marseille en droit des contrats (spéciaux), en droit de la propriété intellectuelle (droit de la propriété littéraire et artistique et droit de la propriété industrielle) ainsi que tutrice dans le cadre du Certificat Internet et Informatique niveau 1. Ses recherches portent sur le droit des affaires et le droit des technologies de l'information, avec un intérêt particulier pour le droit de la gestion électronique des documents en entreprise (sujet de sa thèse).