



Ce document a été publié le 22/02/2012 par **Julie Verdure** sur le site
<http://www.e-juristes.org>.

Il est publié sous licence Créative Commons CC BY-SA 2.0
<http://creativecommons.org/licenses/by-sa/2.0/fr/>

Le concept de « Privacy by Design » : un remède à l'insuffisance des moyens actuels de protection de la vie privée

La protection de la vie privée et des données à caractère personnel est dans tous les esprits. En effet, l'actualité témoigne depuis quelques temps d'une recrudescence d'atteinte à la vie privée des individus. Google a été condamné par la CNIL à une sanction pécuniaire de 100 000 euros le 31 mars 2011¹ pour avoir enregistré des données techniques et personnelles issues de réseaux Wifi mis en place par des particuliers à leur insu par les voitures « Google Cars ». L'objectif de ces voitures est d'enregistrer des vues panoramiques servant à Google Maps et Google Street View. Néanmoins, ces voitures ne faisaient pas qu'enregistrer des vues panoramiques, elles retranscrivaient également des données à l'insu des particuliers, ce qui constitue une véritable atteinte à la vie privée des individus.

Bien entendu, ce phénomène ne connaît pas de frontière : en janvier 2009, l'entreprise Heartland Payment Systems a établi un record peu glorieux, celui de la plus grande perte de données jamais connue, à savoir une perte des données des pistes magnétiques de 130 millions de cartes bancaires. En avril 2011, Sony s'est fait pirater son Playstation network : 77 millions de comptes de joueurs en ligne ont été compromis. La conséquence directe de ces intrusions est que les auteurs de ces piratages peuvent prendre connaissance des noms, adresses postales, emails, mots de passe, identifiants, et données bancaires. En d'autres termes, c'est un accès illimité à toutes les données que chaque individu possède. Cette liste est non exhaustive et des atteintes à la vie privée se produisent chaque jour. Certaines atteintes sont relevées par les autorités de protection des données et nous pouvons en être informés. Mais parfois elles ne le sont pas. Il existe donc de véritables lacunes dans la protection des données à caractère personnel et dans une plus large mesure de la vie privée.

On peut légitimement se poser la question : Comment faire pour résoudre ce problème ? Existe-t-il des solutions pour pallier l'insuffisance des moyens actuels ?

Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada) répond à ces questions par l'affirmative. C'est dans ce contexte qu'elle a proposé un nouveau moyen pour protéger la vie privée. Elle souhaite mettre en place le concept de *Privacy by Design*, concept canadien développé dans les années 90.

Une réponse à des préoccupations nouvelles

Le développement des technologies de l'information, des communications et des réseaux est en plein essor. Les données à caractère personnel sont des données sensibles. Or, grâce aux technologies de plus en plus performantes, il est devenu facile d'accéder à des données autres que les siennes, de les réutiliser et ce notamment à des fins commerciales. Nous sommes actuellement dans un contexte où la technologie dépasse ce que le législateur avait pu imaginer. En conséquence, la protection de la vie privée ne peut plus être assurée par le simple respect des lois et des cadres réglementaires existants.

¹ Source : <http://www.cnil.fr/vos-responsabilites/les-sanctions-de-a-a-z/actualite-sanctions/article/google-street-view-la-cnil-prononce-une-amende-de-100-000-euros/>

C'est donc en réponse à ces nouvelles préoccupations qu'Ann Cavoukian a proposé l'adhésion au principe de « *Privacy by design* ». Il peut se traduire comme étant la protection intégrée de la vie privée dès la conception. Le but de ce principe est d'assurer la protection de la vie privée en l'intégrant dans les normes de conception des technologies, pratiques internes et infrastructures matérielles. La protection intégrée de la vie privée est apparue comme un remède à l'insuffisance de protection de la vie privée actuelle.

Intervenir en amont

Les mesures actuelles de protection de la vie privée sont des mesures « réactives », c'est-à-dire que l'on attend qu'une atteinte à la vie privée ait lieu pour agir. En conséquence, on intervient en aval au lieu d'intervenir en amont pour prévenir l'atteinte. Cette approche est, selon la commissaire Ann Cavoukian, contre productif. Au lieu d'intervenir a posteriori, il faut agir a priori. Les mesures doivent être proactives, c'est-à-dire empêcher l'atteinte de se produire.

Les mesures proposées par l'instauration de ce principe vont plus loin que des mesures légales. Il s'agit véritablement de mettre en place des mesures techniques basées sur sept principes fondamentaux. La protection de la vie privée intégrée est fondée sur le principe selon lequel la technologie est neutre. C'est certes par la technologie que des atteintes à la vie privée ont lieu mais on peut aussi s'en servir pour la protéger.

Un combat contre les « mythes de la protection de la vie privée »

Ann Cavoukian fait état de l'existence de trois mythes concernant la protection de la vie privée :

1. La protection de la vie privée n'existerait plus
2. Plus personne ne se soucierait de la vie privée
3. Plus de sécurité serait égale à moins de vie privée

Le concept de *Privacy by design* veut mettre fin à ses mythes en démontrant que la protection de la vie privée est essentielle. Une étude datant de 2010 réalisée par l'Université de Berkeley² (Californie) a justement mis l'accent sur le besoin de vie privée ressenti par les individus. La majorité des personnes interrogées se sentent aujourd'hui beaucoup plus concernées par les problématiques liées à la vie privée qu'ils ne l'étaient il y a cinq ans. En outre, une importante majorité souhaite voir naître une loi qui imposerait aux sites d'effacer toutes les informations qu'ils possèdent sur les internautes.

En conséquence, il faut combattre ces mythes en démontrant que la protection de la vie privée est essentielle, qu'elle existe, et qu'au contraire, si l'on instaure des règles préalables, c'est-à-dire un peu plus de sécurité, cela reviendrait à mieux protéger sa vie privée. C'est là tout l'engagement d'Ann Cavoukian et l'enjeu du concept de *Privacy by design*.

Quelques exemples concrets

² Source : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

▪ La technologie NFC

La technologie NFC (Near Field Communication) s'apparente à une communication en champ proche. En d'autres termes, il s'agit d'une technologie permettant de communiquer sans fil à courte portée et haute fréquence. Elle autorise l'échange d'informations entre des périphériques distants de 10 cm maximum. Les utilisations sont multiples : un téléphone portable peut se connecter à un ordinateur pour télécharger un fichier, ou encore un appareil photo peut envoyer des images à un ordinateur. Cette technologie peut aller encore plus loin et permettre des achats via son téléphone portable. Bien que cette technologie semble attractive et facilite la vie de tous les jours, il n'en reste pas moins qu'elle présente des risques tant sur le plan de la confidentialité que de la sécurité des données tels que la collecte non désirée de données, la localisation de l'utilisateur, etc.

C'est pourquoi intégrer le concept de *Privacy by Design* dans cette technologie semblerait être une bonne idée et permettrait une meilleure protection de la vie privée des individus. Certains fabricants de téléphonie mobile tentent d'ores et déjà de mettre en place ce mécanisme. Selon Mikko Niva, du Nokia Global Privacy Counsel, la « *protection intégrée de la vie privée est un élément clé de la stratégie de Nokia en matière de confidentialité et elle constitue un engagement dans le cadre du processus de création de ses produits* ».

▪ Le Smart Grid

Le *Smart Grid* est un réseau de distribution d'électricité « intelligent ». Il utilise la technologie informatique afin d'optimiser sa production et sa distribution d'électricité. Les objectifs principaux de cette technologie consistent à économiser l'énergie, sécuriser le réseau et réduire les coûts. Il s'agit également de mieux adapter la distribution de l'électricité en fonction des besoins des consommateurs et ainsi trouver un équilibre entre l'offre et la demande.

Bien que peu connue en France, cette technologie est à la pointe aux Etats-Unis et présente des dangers en matière de protection de la vie privée. Cette nouvelle technologie informatique, en permettant de collecter des données sur la consommation d'électricité de chaque foyer, détermine le nombre approximatif d'occupants, s'ils sont présents, éveillés, endormis, la fréquence des douches, etc. Ann Cavoukian en a fait son cheval de bataille.

" *Le seuil de tolérance est atteint* ", déclare la Commissaire Cavoukian avec insistance. " *Il est maintenant temps d'aborder ce problème, tant que le Smart Grid en est toujours à ses balbutiements, et tant que les services publics s'efforcent de maintenir la base existante de confiance des consommateurs qui sera essentielle à la réussite du futur Smart Grid.* »

Sur le court terme, intégrer le concept de *Privacy by Design* dans les technologies, c'est prévenir les atteintes à la vie privée. Sur le long terme, c'est à la fois protéger la vie privée et finalement permettre un usage plus sécurisé et plus serein des technologies qui commencent à effrayer certains utilisateurs.

Un avenir prometteur

Les enjeux qui se cachent derrière la protection de la vie privée sont importants. C'est la raison pour laquelle ce concept fait l'objet d'une attention particulière des pouvoirs publics et des autorités de contrôle. Ce concept est reconnu tant à l'échelle européenne qu'à l'échelle française. Dès le 26 mars 2009, le parlement européen dans une recommandation à l'attention du Conseil a voulu promouvoir la mise en œuvre du principe « Privacy by Design », selon lequel « *la protection des données et de la vie privée devrait être introduire dès que possible dans le cycle de vie des nouveaux développements technologiques, assurant aux citoyens un environnement convivial* ³ ».

En mai 2010, le contrôleur européen de la protection des données, Peter Hustinx, a insisté sur la nécessité d'intégrer les principes de *Privacy by Design* dans les technologies de l'information et de la communication⁴. C'est ensuite le 4 novembre 2010 que s'est poursuivie la reconnaissance de la protection intégrée de la vie privée dans le considérant 46 de la révision de la directive du 24 octobre 1995, Directive 95/46/CE, qui fait état de la nécessité de prendre des mesures « *tant au moment de la conception qu'à celui de la mise en œuvre du traitement* ⁵ ».

Cette reconnaissance progressive du concept de *Privacy by Design* s'est achevée par la consécration du principe lors de la 32^{ème} conférence internationale des commissaires à la protection des données et de la vie privée qui a eu lieu en 2010 à Jérusalem. Une résolution a été adoptée à l'unanimité reconnaissant le concept de la vie privée dès la conception en tant qu'« *élément essentiel de la protection fondamentale de la vie privée* ⁶ » et soulignant l'importance de prendre en compte la vie privée dès la conception.

Au niveau national, un rapport du groupe « Droit à l'oubli numérique » de Cyberlex du 25 mai 2010⁷ a encouragé la mise en œuvre du concept de *Privacy by Design*. Le 22 juin 2011, un rapport de l'Assemblée nationale sur les droits de l'individu dans la révolution numérique⁸ a prévu une orientation visant à faire du *Privacy by Design* un atout majeur pour l'Europe.

Des difficultés à résoudre

Ce concept, devenu un véritable principe reconnu au niveau mondial, reste cependant flou pour la plupart. On comprend son importance, mais on ne voit pas comment mettre en place un tel mécanisme. La difficulté réside dans le fait que ce concept se situe à la frontière entre la technique et le droit. Les juristes n'ont pas toujours les capacités techniques pour comprendre le fonctionnement de ce concept tandis que les spécialistes de la technologie, les ingénieurs, n'ont pas forcément connaissance des enjeux juridiques qu'il y a derrière la mise en place d'une telle technologie.

³ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:117E:0206:0213:FR:PDF>

⁴ http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newslatters/Newsletter_24_FR.pdf

⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:NOT>

⁶ <http://www.justice.gov.il/NR/rdonlyres/3FB67FDB-92DF-4DA0-9146-371DC1992F25/26502/ResolutiononPrivacybyDesign.pdf>

⁷ <http://www.cyberlex.org/page-accueil/cyberlex-remet-son-rapport-droit-a-loubli.html>

⁸ <http://www.assemblee-nationale.fr/13/rap-info/i3560.asp>

Aussi, il est nécessaire pour le développement de ce principe que les autorités de protection des données et les acteurs de l'industrie du numérique travaillent ensemble pour atteindre un unique objectif : la protection de la vie privée et des données à caractère personnel.

Vers un nouveau principe, corolaire du principe de Privacy by Design

Christian Pardieu, counsel, Europe Privacy Leader and Gouvernement Affaires & Polyce, GE, a évoqué le terme de « *Privacy by Redesign* ». Ce principe aurait pour objectif de mettre en conformité les outils existants. A la différence du principe de *Privacy by Design* qui intervient dès la conception, *Privacy by Re-design* est une nouvelle approche qui viserait à appliquer les principes fondamentaux de Privacy by Design aux systèmes existants.

On ne connaît pas encore la portée de ce principe et il semble encore plus difficile à mettre en œuvre que le concept de *Privacy by Design*. Néanmoins, son apparition démontre bien que la protection de la vie privée est de plus en plus au cœur des préoccupations et que le concept de *Privacy by Design* a encore de beaux jours devant lui. La protection de la vie privée intégrée dès la conception est une notion qui devient de plus en plus populaire et qui semble apporter une réponse concrète aux problématiques que posent les nouvelles technologies.

Julie Verdure



Pour aller plus loin :

- <http://privacybydesign.ca/>
- <http://www.youtube.com/watch?v=h4mSjD0XXwg>