Futur Règlement européen sur la protection des données, qui est concerné ?

Futur Règlement européen sur la protection des données, qui est concerné ?

Le 25 février dernier, Arendt & Medernach organisait une conférence sur le futur Règlement européen sur la protection des données (ci-après « le Règlement »[1]afin de permettre aux entreprises de mieux comprendre les nouvelles obligations auxquelles elles seront prochainement soumises et leur procurer l'essentiel de ce qu'il faut retenir de ce nouveau texte.

Contexte

Après deux années riches en actualités en matière de données personnelles (droit à l'oubli consacré par la Cour de Justice de l'Union européenne (CJUE)[2], et invalidation du Safe Harbor[3] notamment), le nouveau Règlement arrive à point nommé pour remplacer le cadre juridique actuel adopté il y a plus de 20 ans[4].

4 ans de discussions et 4000 amendements ont été nécessaires pour parvenir à un accord autour de ce nouveau texte qui sera adopté en mai/juin prochain. Il sera applicable dans deux ans à compter de sa date d'entrée en vigueur, soit pour l'été 2018.
Si l'échéance semble lointaine, il est toutefois nécessaire d'envisager dès à présent les changements apportés par ce nouveau texte.

De nouvelles obligations pour les entreprises

Il résulte de ce Règlement diverses obligations pour les entreprises et notamment :

• De mettre en œuvre les principes de « privacy by design / privacy by default» afin d'assurer une protection des données dès leur conception et par défaut ;
• De tenir des registres des traitements de données personnelles sauf cas exceptionnels ;
• De notifier toute violation de données dans les 72h auprès de l'autorité de contrôle voire de la personne concernée le cas échéant ;
• De détailler/préciser l'information des personnes concernées ;
• D'adapter leurs contrats de sous-traitances ;
• D'assurer la portabilité des données ;
• De nommer un Délégué à la Protection des Données le cas échéant.
• Les entreprises doivent envisager ces obligations avec le plus grand sérieux puisque de nouvelles sanctions financières pourront désormais être prononcées par les autorités nationales de protection des données. En effet, selon le manquement, ces sanctions pourront atteindre de 2 à 4% du chiffre d'affaires mondial d'une entreprise ou de 10 à 20 millions d'euros, le montant le plus important devant être retenu.

Qu'est-ce qu'une donnée personnelle ?

"Les données à caractère personnel sont définies par le futur Règlement comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement , notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale ».
Cette définition est identique à celle prévue actuellement dans la loi luxembourgeoise[7] mais elle ajoute quelques exemples. Il est notamment précisé qu'un identifiant en ligne, tel qu'une adresse IP, peut être qualifié de données à caractère personnel," explique Héloïse Bock, Partner Arendt & Medernach.

Est-ce qu'on peut dire que toutes les entreprises seront concernées par ce nouveau Règlement ?

"Le champ d'application du règlement est élargi puisque celui-ci aura vocation à s'appliquer à toutes les entreprises traitant des données personnelles dès lors qu'elles sont établies sur le territoire de l'Union européenne ou, lorsqu'elles sont établies hors de l'Union européenne si ces traitements ciblent des citoyens européens.
Un grand nombre d'entreprises seront ainsi concernées en pratique," poursuit-elle.

Des droits nouveaux et renforcés

Pour les personnes concernées, ce nouveau Règlement introduit le célèbre droit à l'oubli ou droit à l'effacement, déjà consacré par la CJUE en 2014[5] mais également, le droit à la portabilité des données qui permet de transférer les données d'un prestataire vers un autre. Les droits d'accès, d'opposition et de rectification des données ainsi que le droit à l'information, existants dans le cadre juridique actuel, sont maintenus et renforcés.

Les transferts de données hors de l'Union européenne

Concernant les transferts de données en dehors de l'Union européenne, le Règlement ajoute de nouvelles bases de légitimité ponctuelles/limitées sur lesquelles un responsable de traitement pourra se fonder en cas de transfert vers un pays n'assurant pas un niveau de protection adéquat.
Le sort des transferts de données réalisés vers les Etats-Unis n'est pas réglé par le Règlement, toutefois, une nouvelle décision d'adéquation est attendue très prochainement[6]. La Commission européenne et les États-Unis se sont en effet accordés sur un nouveau cadre pour les transferts transatlantiques de données le mois derniers : le «bouclier vie privée UE-États-Unis» ou « EU-US Privacy Shield ».

To do list avant 2018

Pour conclure, les avocats d'Arendt & Medernach ont dressé une « to do list » générale reprenant les points suivants :

• Recenser les traitements de données réalisés en pratique et leurs finalités;
• Faire un audit pour évaluer le niveau de conformité actuel et identifier les lacunes;
• Réaliser un « mapping » de tous les transferts de données en considérant les catégories de données, les destinataires des transferts, les bases de légitimité etc.;
• Effectuer des études d'impact lorsqu'un traitement à risque est envisagé;
• Nommer un délégué à la protection des données si nécessaire;
• Mettre en place ou adapter la documentation existante (registres, policies, contrats de sous-traitance, etc.)

[1] 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) (2012/0011 COD)
[2] CJUE, 13 mai 2014, affaire C-131/12
[3] CJUE, 6 octobre 2015, affaire C-362/14
[4] 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
[5] CJUE, 13 mai 2014, affaire C-131/12
[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
… [Lire la suite]

Réagissez à cet article

Source : *Futur Règlement européen sur la protection des données, qui est concerné ?*

La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende

La Cnil pourra infliger jusqu’à 20 millions d’euros d’amende

Pourtant hostile au départ, le gouvernement est désormais favorable à un renforcement du pouvoir de sanction de la Cnil : jusqu'à 20 millions d'euros en cas de récidive. Et la portabilité des données ? « Ce sont les gros qui sont énervés » répond Axelle Lemaire.

Le projet de loi République numérique présenté par Axelle Lemaire est actuellement débattu par les députés. De nombreux amendements sont à l'étude, dont certains rejetés par le gouvernement. Celui-ci s'est en revanche rallié à une proposition des parlementaires en faveur d'un renforcement du pouvoir de sanction de la Cnil, l'autorité en charge de la protection des données personnelles.
Selon Les Echos, le gouvernement soutient donc désormais un amendement prévoyant, en cas de récidive, de permettre à la Cnil d'infliger une sanction pouvant atteindre jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. A ce jour, en cas de récidive, la sanction ne peut pas dépasser les 300.000 euros.

Les « gros » sont « énervés »

Une autre mesure portant sur les données fait grincer des dents au sein de plusieurs organisations d'entreprises du numérique : la portabilité des données entre plateformes.
« Par son caractère large, il impose des contraintes extrêmement lourdes à des secteurs dans lesquels la portabilité n'apporte pas d'intérêt du point de vue des consommateurs et sur le plan de la concurrence. En l'état, il menace directement les investissements massifs réalisés par les entreprises du secteur afin d'améliorer leurs services » dénonçaient-elles notamment dans un communiqué du 14 janvier.
Message reçu au sein du gouvernement ? Difficile à dire puisque la ministre du numérique déclarait lundi 18 janvier sur RMC vouloir « protéger la concurrence ». « Ce sont les gros qui sont énervés, pas les petits » ajoutait-elle.

Réagissez à cet article

Source : *La Cnil pourra infliger jusqu'à 20 millions d'euros d'amende*

Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises | Le Net Expert Informatique

	**Nouveau règlement européen sur la protection des données personnelles : Les changements pour les entreprises**

Fin juillet, le Contrôleur Européen de la Protection des Données a publié ses recommandations sur le futur règlement européen portant à quatre le nombre de versions du document. L'occasion de faire le bilan sur les trois évolutions du règlement qui auront le plus d'impact pour les entreprises.

QUEL CHANGEMENT POUR LES ENTREPRISES ?

Mise en place du Privacy by Design (Articles 23, 30, 32a, 33a et 33)

Première nouveauté, les entreprises devront définir et mettre en œuvre des procédures permettant d'intégrer les problématiques liées à la manipulation des données personnelles dès la conception de nouveaux services.

Cette démarche s'accompagne de l'obligation de réaliser des analyses de risques relatives à la vie privée des personnes (discrimination, diffusion de données confidentielles, etc.) préalablement à la mise en place des traitements les plus sensibles et à chaque modification du traitement.

Face aux risques sur la vie privée des personnes induits par ces traitements, il sera imposé aux entreprises d'adopter des mesures de sécurité adéquates en vue de les maitriser.

Concrètement que retenir du Privacy by Design ?

Une mise à jour de la méthodologie projet afin d'identifier au plus tôt les traitements sensibles et une méthode d'analyse de risques à définir et outiller.

Il sera pour cela possible de s'inspirer des guides pratiques de la CNIL intitulés « Etude d'impact sur la vie privée », qui seront à simplifier et contextualiser aux besoins spécifiques de l'entreprise.

Responsabilisation ou « Accountability » (Articles 22 et 28)

Toute entreprise devra désormais être capable de prouver sa conformité vis-à-vis du règlement.

Cette exigence se traduit par :

• l'adoption d'une politique cadre de gestion des données à caractère personnel ;

• une organisation associée ;

• des procédures opérationnelles déclinant les thèmes du règlement (information, respect des droits des personnes, transfert à des sous-contractants, etc.).

L'entreprise devra également être en capacité de prouver l'application de ces politiques et donc, de mettre en place des processus de contrôle.

L'occasion de parler de la personne qui illustrera ce principe d' « Accountability » : le DPO (pour Data Protection Officer). Il devient quasiment obligatoire et remplace le CIL actuel.

Concernant ce DPO, le texte entérine l'obligation de lui fournir le personnel, les locaux, les équipements et toutes les autres ressources nécessaires pour mener à bien ses missions. Encore une fois le parlement souhaite aller au-delà de cette exigence : il propose de nommer au sein de la direction une personne responsable du respect du règlement.

Comment appliquer ce principe ? Il sera nécessaire de définir a minima une politique avec des règles de protection des données ainsi qu''un plan de contrôle et de formation. Cette politique pourra par exemple s'inspirer du modèle des BCR « Binding Corporate Rules », dont le principe a été entériné dans le futur texte, pour lesquelles des modèles types et des premiers retours d'expérience existent déjà.

Obligation de notification des fuites (articles 31 et 32)

L'ensemble des parties s'accordent sur l'obligation de notification des fuites aux autorités. Le Parlement propose même que les entreprises mettent en ligne un registre listant les types de brèches de sécurité rencontrées. Il sera intéressant de constater comment cette exigence cohabitera avec les législations nationales en matière de sécurité et la protection des intérêts de la nation qui tendent à limiter la diffusion de ce type d'information.

La notification de fuites aux personnes concernées, quant à elle, n'est obligatoire que si l'entreprise n'est pas en mesure de démontrer qu'elle a mis en œuvre des mesures afin de rendre cette fuite sans conséquence. D'où l'intérêt d'effectuer correctement l'analyse de risques, de définir et d'implémenter des mesures appropriées.

Au final, deux recommandations afin d'anticiper le futur règlement sur ce point :

• un processus de gestion des fuites de données à définir en l'orchestrant avec les dispositifs de gestion de crise existants et les processus de relation client,

• la réalisation d'exercices réguliers afin de tester son efficacité avec tous les acteurs concernés.

UNE MISE EN CONFORMITÉ À ANTICIPER

Au-delà de ces trois nouveautés majeures, d'autres modifications plus limitées en termes d'impacts organisationnels sont également à prendre en compte, comme la création du droit à la portabilité ou l'extension de la liste des données sensibles. On peut par ailleurs noter le renforcement d'obligations existantes comme le droit à l'information et le recueil du consentement. Le diable se nichera dans les détails.

Pour conclure, les deux années de mise en application du règlement ne seront pas de trop (soit une mise en conformité d'ici début 2018) et nous ne pouvons que conseiller d'initier la mise en conformité dès 2016, avec le cadrage et le lancement des premiers chantiers majeurs. D'autant plus que le sujet devient de plus en plus visible médiatiquement (condamnation récente de Boulanger, Google et l'application du droit à l'oubli, etc.) et que les sanctions financières deviennent réellement significatives (entre 2 et 5% du chiffre d'affaire mondial). L'occasion pour toutes les entreprises de communiquer largement sur les principes de respect de la vie privée effectivement appliqués.

Source : http://www.solucominsight.fr/2015/09/nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-anticiper-les-3-impacts-majeurs/

Les objets connectés deviendraient des témoins ? | Le Net Expert Informatique

Les objets connectés deviendraient des témoins ?

Aux Etats-Unis, on commence à produire les données de bracelets connectés pour démentir ou renforcer un témoignage. Ces données pourraient aussi entrer dans nos tribunaux, ce qui n'est pas sans poser question.

À quoi servent les objets connectés « portables », ces bracelets ou ces montres qui permettent de mesurer votre activité physique, vos dépenses en calories et même parfois votre humeur ?
À mieux se connaître, répondent les amateurs. À mener une vie plus saine. Mais une histoire récente, aux Etats-Unis, montre que ces objets peuvent aussi servir lors de votre procès.

Et là, son FitBit a lâché le morceau
Une femme de 43 ans qui avait porté plainte pour viol a été démentie par les données de son FitBit (bracelet connecté mesurant l'activité et le sommeil). L'histoire a été rapportée la semaine dernière par la chaîne d'information locale ABC 27 News.
La femme avait affirmé aux enquêteurs qu'un homme s'était introduit au milieu de la nuit dans sa chambre et l'avait menacée avec un couteau avant de la violer. Mais son gadget a contesté ses dires :
« Elle avait affirmé qu'elle avait perdu sa montre de fitness en résistant à son agresseur, mais l'objet a été retrouvé intact dans le couloir, près de la salle de bains [où elle avait dit que s'était déroulé le viol, ndlr].
Selon le chef d'inculpation, quand les enquêteurs ont téléchargé son activité de fitness, ils se sont aperçus que la femme n'avait pas dormi cette nuit-là et qu'elle avait marché tout le temps, au lieu de dormir comme elle l'avait affirmé. »
En plus de ces données, les enquêteurs n'ont trouvé aucune trace de pas dans la neige autour de la maison (les faits se sont déroulés en mars) ni aucune trace d'intrusion. En conséquence, la femme a été inculpée pour fausse déclaration et altération de preuves.

Des grosses balances, ces Google Glass
Déjà, en novembre 2014, à Calgary (Canada), une femme, qui demandait à être indemnisée pour préjudice corporel après un accident, a utilisé les données de son bracelet connecté pour prouver que son activité physique était réduite depuis son accident. (Une histoire alors analysée par Olivier Ertzscheid.)

Les objets connectés arrivent donc dans les tribunaux. Et selon les avocats cités dans la presse américaine (ici ou ici, par exemple), cette tendance est appelée à grandir. Dans Wired, un avocat américain se demandait ainsi :
« [Les données des objets connectés] pourraient-elles être utilisées comme alibi ? »
Ou encore :
« Est-ce qu'on pourrait utiliser les données d'un FitBit pour prouver qu'un cardiologue avait fait preuve de négligence, en ne restreignant pas l'exercice d'un patient ? »
Ces objets peuvent donner des indications sur les activités de celui ou celle qui le porte, mais aussi sur le lieu où il ou elle se trouve, grâce à des fonctions de géolocalisation. Les plus sophistiqués, comme les Google Glass, font aussi des photos ou des vidéos, ainsi que des recherches sur le Web.
On voit bien l'usage que policiers, assureurs ou autres pourraient faire de ces données, en les retournant contre son propriétaire.

Bientôt dans nos prétoires
En France, le cas ne s'est encore jamais présenté, mais, explique Me Clarisse Le Corre, avocate au cabinet Vigo, il est tout à fait envisageable :
« Selon la loi, les infractions peuvent être établies par tous modes de preuve et c'est le juge qui décide ensuite selon son intime conviction. »
A cheval entre données personnelles et données médicales, ces informations sont souvent appelées « données de bien-être ». Elles sont protégées par la loi « Informatique et libertés », mais dans le cas d'un procès, cette protection peut être levée par l'instruction.
Pourvu qu'elles soient légalement recevables et qu'elles soient ensuite soumises au contradictoire, c'est-à-dire être débattues par les deux parties, les données des objets connectés peuvent tout à fait être présentées devant un tribunal.

Leurs données sont-elles fiables ?
Pourtant, ces données sont loin d'être totalement fiables.
Les objets connectés buguent.
Comme l'a récemment montré notre collègue Thibaut Schepman, les appareils connectés peuvent buguer et les données récoltées ne reflètent pas forcément vos activités.

Ils sont faciles à duper.
Pas besoin de réfléchir longtemps pour voir comment on pourrait duper le bracelet connecté : il suffit de le faire porter par un complice ou de l'apposer à un animal domestique au comportement pas trop erratique. Ou encore de rester assis à son bureau en bougeant les pieds très vite pour faire croire qu'on fait un jogging.

Ils « mesurent » selon des critères qui changent de machine en machine et sont déterminés par des algorithmes inaccessibles.
Comme le rappelle la chercheuse américaine Kate Crawford dans The Atlantic, les mesures qu'effectuent ces outils dépendent de la façon dont ils ont été programmés et sont souvent imprécises.

« Le Jawbone UP, Nike Fuelband, FitBit and Withings Pulses [différents modèles de bracelets connectés, ndlr] ont chacun des modes de fonctionnement particulier : certains comptabilisent les mouvements de bras comme de la marche (merveilleux, si vous voulez comptabiliser l'écriture comme de l'exercice), d'autres comptabilisent difficilement le vélo comme une activité physique.

La fonction de mesure du sommeil emploie des méthodes assez grossières pour faire la différence entre sommeil léger et sommeil profond. […] »

Un bracelet Jawbone Up (Ashley Baxter/Flickr/CC)

La chercheuse ajoute, faisant référence à l'exploitation de ces données :
« Ces données sont rendues encore plus abstraites par des entreprises d'analytique qui créent des algorithmes propriétaires, pour les comparer à leur standard de ce qu'est une personne normale "en bonne santé." »

Effectivement, explique Me Le Corre, à mesure que l'on s'interroge sur le statut de ces objets, on découvre leurs limites :

« La question de la fiabilité des données de ces objets va se poser de façon aiguë. Pour l'instant, nous manquons de recul sur ces choses-là parce qu'elles sont très récentes. D'où l'intérêt de le soumettre à la discussion des deux parties, qui sert de garde-fou. »

Les données par elles-mêmes ne signifient rien : elles s'intègrent dans un faisceau de preuves, et doivent toujours être contextualisées.

Au-dessus des témoins humains…
En voyant les données de bien-être utilisées contre leur propriétaire, on comprend aussi mieux ce que sont vraiment les objets connectés.
Ainsi, réfléchissant sur ce thème, la chercheuse Kate Crawford, qui travaille sur les implications du big data et des objets connectés, rappelle l'ambiguïté fondamentale des objets connectés :

– ils se présentent comme les instruments d'une meilleure connaissance de soi,
– mais sont aussi des « informateurs », qui collectent des données et les transmettent au fabricant et à des tiers – potentiellement à des assureurs et des employeurs.
Plus profondément, c'est le statut que l'on veut donner à ces données qui est en jeu. Kate Crawford met en garde contre la tentation d'une « vérité fondée sur les données », où celles-ci finiraient par sembler plus fiables – parce que plus neutres – que l'expérience des témoins.

« Donner la priorité aux données, qui sont irrégulières et peu fiables, sur les témoignages humains, cela signifie que l'on donne le pouvoir à l'algorithme. Or ces systèmes sont imparfaits – comme peut l'être le jugement humain. »

Les données des objets connectées ne sont que ça, des données : des mesures qu'il faut contextualiser et comprendre, et surtout ne pas prendre pour argent comptant.

Source : http://rue89.nouvelobs.com/2015/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-260040

Les entreprises doivent construire un modèle d'exploitation de leurs données

Les entreprises doivent construire un modèle d'exploitation de leurs données

Face au Big Data, monétisation, confidentialité et gouvernance sont au menu des préoccupations des entreprises françaises en 2015.

En 2014 déjà, 43% des décideurs français interrogés considéraient la gestion des données et leur analyse comme une priorité selon une étude réalisée par MARKESS*. Aujourd'hui, les directions générales de nombreuses entreprises françaises le clament : l'année 2015 sera l'année du Big Data. Dans le rapport Data & Analytics Trends 2015 élaboré par le cabinet Deloitte, ces dernières voient en effet se dessiner un grand potentiel économique derrière la masse de données qu'elles génèrent. Les sociétés ressentent le besoin d'analyser les données qu'elles collectent pour créer de la valeur : anticiper des événements futurs, gérer les ressources, limiter les risques voilà autant de finalités à l'exploitation de ces données pour l'entreprise. Reste à savoir comment les exploiter au mieux. Et les solutions technologiques ne manquent pas.

En milieu hospitalier notamment, où l'expérience du patient occupe une place centrale, rassembler des données, sous la forme d'un tableau de bord offrant une visualisation modulable de l'information, sur les temps d'attente des patients ou encore les facteurs d'attribution d'une chambre, peuvent permettre au personnel infirmier, aux médecins et aux administrateurs d'optimiser leur capacité de traitement des patients, note Edouard Beaucourt, account manager chez Tableau Software.

L'Open Data, soit le partage de données, reçoit un écho favorable auprès des acteurs du secteur privé et ceci à des fins d'amélioration de la qualité des services offerts. Deloitte constate d'ailleurs une recrudescence des actions collaboratives entre les sociétés et leurs partenaires en matière de partage de données. Et plusieurs discussions naissent autour de la création de centres de partage de données inter-entreprises. Ce processus de démocratisation du partage de données encore faiblement structuré est amené à se rationaliser selon Reda Gomery, spécialiste des données et de l'analyse de données chez Deloitte, auteur de l'étude.

Preuve de l'émergence d'une collaboration accrue entre les parties prenantes, Deloitte relève le projet d'une compagnie d'assurance, l'«hackathon », compétition ouverte aux développeurs de tous horizons. Leur mission consiste à réfléchir à de nouvelles applications de scoring des clients de l'entreprise à partir de données qui leur sont confiées.

Il est d'usage de dire que les crises s'accompagnent souvent d'un regain de créativité. Raison pour laquelle les entreprises cherchent une monétisation adéquate de leurs données. Les secteurs des télécoms et des services financiers ont été d'ailleurs été pionniers dans le développement de services de vente de données.
Deloitte met en avant dans son rapport l'initiative d'un opérateur téléphonique qui d'après les données fournies par ses antennes relais a su analyser la fréquentation de sites touristiques par des visiteurs étrangers, données qui ont pu être vendues par la suite à des offices de tourisme, générant ainsi de nouveaux revenus pour l'entreprise.

En 2015, les entreprises réalisent complètement la valeur des informations qu'elles possèdent pour les acteurs avec qui elles interagissent et expérimentent de nouveaux modèles. Non sans interrogations sur la confidentialité de ces données. Se pencher sur les modèles de protection pour sécuriser l'information et préserver l'anonymat des clients conduit à son corollaire : le mode de gouvernance. Les entreprises se préoccupent en effet également de chercher le cadre le plus adapté pour maîtriser ses flux gigantesques et continus d'informations.

*Etude MARKESS : Meilleures approches pour tirer parti du Big Data, France, 2014

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atelier.net/trends/articles/entreprises-doivent-construire-un-modele-exploitation-de-leurs-donnees_433304

Protection de la vie privée : pas avant 2025, au mieux !

Protection de la vie privée : pas avant 2025, au mieux !

Une étude menée par Pew Research Center a posé la question a plus de 2500 experts et politiciens sur la création d'un cadre unique pour garantir la protection des données privées tout en facilitant l'innovation et le business des entreprises.

Le Pew Research Center a mené une enquête originale pour connaître l'opinion de plus de 2500 experts techniques et des politiciens sur l'avenir du respect de la vie privée. Concrètement, l'étude s'interrogeait sur la capacité des législateurs et développeurs à créer un cadre capable de garantir la vie privée d'ici 2025. Ce cadre devra à la fois simplifier l'innovation et la monétisation des applications, tout en offrant aux utilisateurs des options de sauvegarde de leurs données personnelles.
L'opinion des experts est divisée. 55% des répondants ne croient pas qu'un tel cadre puisse voir le jour dans la prochaine décennie. Mais 45% sont plus optimistes sur sa création et son acceptation. Par ailleurs, si les avis sont tranchés sur l'avenir de la confidentialité des données personnelles, il existe un consensus pour souligner que la vie en ligne est par nature publique. Il s'agirait donc bien d'un problème d'éducation de l'utilisateur, mais aussi du comportement des sites qui promettent plus de facilité contre des informations privées. L'étude qui cite Bob Briscoe, chercheur sur l'infrastructure et le réseau chez British Telecom, estime que cette facilité et ce confort sont à l'origine de l'absence de préoccupations des utilisateurs sur leurs données personnelles.

Un souci de définition, des outils de chiffrement nécessaires
Pour Joe Wilbanks, responsable de Sage Bionetworks revient sur le cadre général en constatant que 10 ans c'est trop court pour le législateur d'ajuster les règlements face à la rapidité des évolutions technologiques. D'autres comme Nick Arnett, expert en BI chez Buzzmetrics, confie que les définitions de « liberté » et de « vie privée » vont changer dans la société d'ici 2025 et il y aura souvent des désaccords sur ces transformations. Idem pour Homero Gil de Zuniga, directeur de recherche Digital Media à l'Université du Texas à Austin qui pense que « l'information sera encore plus omniprésente, plus fluide et portable. Les sphères publiques et privées numériques vont probablement se chevaucher ». Ce qui lui fait dire que ce qui est privé aujourd'hui ne le sera peut-être pas demain.
Peter Suber, directeur d'un projet d'accès illimité à la recherche (Open Access), prévient que pour créer un cadre unifié et acceptable, il y aura au préalable une course aux technologies qui favorisent la vie privée et la sécurité. Il ajoute que cette phase est en cours aujourd'hui avec le développement du chiffrement. Il reste des efforts à mener néanmoins sur la sécurité des données personnelles qui n'est pas du seul fait des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.silicon.fr/donnees-personnelles-un-cadre-unique-en-2025-est-il-utopique-104490.html
Par Jacques Cheminat

Du « Privacy by Design » aux Privacy Rules : accompagner et encadrer le développement des usages autour de la biométrie – JDN Web & Tech

Du « Privacy by Design » aux Privacy Rules : accompagner et encadrer le développement des usages autour de la biométrie

On assiste, depuis quelques mois, à un développement de nouveaux usages de la biométrie, utilisée à des fins de sécurité, dans le cadre d'applications de paiement et de signature électronique, d'authentification en proximité et en ligne…

Cette utilisation de la biométrie s'inscrit dans une logique d'authentification permettant de vérifier que le possesseur du support personnel est « bien le bon titulaire ». Celle-ci se retrouve dans les recommandations émises dans le rapport sur l'avenir des moyens de paiement en France, et la nécessité d'«identifier les évolutions nécessaires des moyens de paiement existants et les innovations qui permettraient d'en créer de nouveaux afin de mieux satisfaire les besoins des consommateurs et des entreprises toutes en améliorant la sécurité et en réduisant les coûts pour l'ensemble des parties prenantes, et ce de manière équitable ».Il s'agit en effet de répondre aux besoins croissants d'une méthode d'authentification simple, universelle et sécurisée, qu'entrainent la dématérialisation croissante des transactions et la multiplication des canaux de distribution (automates bancaires, téléphones et tablettes…).

La frontière devient de plus en plus ténue entre moyen de paiement et moyen d'acceptation
Mais au-delà de la finalité, c'est l'implémentation qui permet de définir un certain niveau de sécurité, d'instaurer la confiance et donc l'appropriation de la technologie. Ainsi une implémentation à des fins de sécurité doit prendre en compte différents paramètres comme l'utilisation d'au moins 2 facteurs, dont un support personnel permettant à l'utilisateur « la maîtrise de sa donnée biométrique ». Ce support assurera le stockage sécurisé des données biométriques et l'exécution des applications (dont l'algorithme de comparaison et les applications reposant sur l'authentification).

Une implémentation appropriée de la biométrie permet d'en garantir l'intégrité et la sécurité et donc la protection de ses données personnelles. Natural Security qui a été distingué en 2013 « Privacy by Design ambassador », a inscrit les problématiques de protection des données personnelles et de la vie privée dés le commencement de ses travaux en 2008. Le PbD, sans être une norme, vise à instaurer un état d'esprit en s'appuyant sur un certain nombre de grands principes . Cette démarche est en parfaite cohérence avec une démarche de type Privacy Impact Assessment qui apparaît à ce regard plus formelle et va tendre à se généraliser en Europe.

La démarche de Privacy By Design trouve un écho tout particulier en Europe où, dés 2005, « les données biométriques qui sont uniquement utilisées à des fins de vérification devraient être stockées de préférence sur un support individuel sécurisé, par exemple, une carte à puce par exemple, que détiendrait la personne concernée ». Le standard définit par Natural Security repose sur des spécifications ouvertes à tous les industriels. Ce choix d'ouverture permet la mise en place d'un schéma d'évaluation et de certification permettant de vérifier que les implémentations ont été effectuées dans le respect des règles et des valeurs qui structurent ce standard. S'il s'agit de vérifier l'interopérabilité entre les différentes implémentations effectuées par les industriels, la démarche de certification vérifie quant à elle que les règles de sécurité et de protection des données personnelles ont bien été implantées.
Dans ce prolongement, des règles de conformité, les « Privacy Rules » viennent compléter le dispositif en engageant le responsable de traitement à une utilisation respectueuse de la protection des données personnelles, afin d'éviter, par exemple, la constitution de base de données biométriques.

D'autres dimensions de l'utilisation de la biométrie restent à discuter. Leur évaluation reste un point clé. On peut souligner le projet de la Biometrics Alliance Initiative , financé par des fonds européens, qui vise à développer un référentiel d'évaluation des technologies biométrique, dans le champ non-régalien afin de définir ce qu'on est en droit d'attendre en termes de performances, d'interopérabilité et de sécurité.

L'utilisation de la biométrie dans un contexte d'authentification constitue un des enjeux d'aujourd'hui pour l'accès aux services et la réalisation de transactions. La démarche de Privacy by Design est une invitation à intégrer la dimension sociale dans la conception d'une technologie. Elle devient dés lors une caractéristique à part entière « Not just good business, but good for business ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/ebusiness/expert/59177/du–privacy-by-design–aux-privacy-rules–accompagner-et-encadrer-le-developpement-des-usages-autour-de-la-biometrie.shtml
Chronique de André Delaforge