Les entreprises françaises bientôt condamnées à changer leur système de traitement des donnée personnelles ?

Les entreprises Françaises bientôt condamnées à modifier leur système de traitement des données personnelles ?

L'échéance se rapproche dangereusement. A partir de la fin du mois de janvier, entreprises américaines et européennes ne pourront plus faire circuler de données de part et d'autre de l'Atlantique.

Le 6 octobre 2015, la Cour de justice européenne a en effet rendu une décision invalidant le « Safe Harbor », ce traité transatlantique sur le transfert des données personnelles. Premiers touchés, les géants américains du numérique, comme Facebook, Google ou Microsoft, qui exploitent massivement les donnes personnelles.

Qu'en est-il des entreprises françaises qui, sans toujours le savoir, communiquent les données personnelles de leurs clients. De leurs salariés, de leurs contacts… sur des serveurs aux États Unis ? (Gmail, DropBox, Google Drive…)

A partir de la fin du mois de janvier, les entreprises américaines et européennes, et donc françaises, ne pourront plus faire circuler de données de part et d'autre de l'Atlantique.

Vous avez des doutes, vous souhaitez être accompagné ?

contactez-nous

Réagissez à cet article

Source : *Fin du « Safe Harbor » : Gattaz tire la sonnette d'alarme*

Est-ce que la réutilisation de données personnelles sera possible dans le nouveau Règlement vie privée ?

Est-ce que la #réutilisation de données personnelles sera possible dans le #nouveau Règlement vie privée ?

Tout praticien de la protection des données personnelles a déjà été confronté au problème du changement de finalité d'utilisation des données. Exemple : elles ont été collectées pour une finalité d'exécution d'un service en ligne (accès à un réseau social ou livraison d'un bien acheté) et on voudrait aujourd'hui les vendre en vue d'alimenter une processus de profilage big data. Les conditions de pareils changements de finalité ont divisé les juristes et organes de contrôle depuis la directive de 1995. Le nouveau règlement semble avoir tranché : la poursuite d'une nouvelle finalité incompatible avec la première est interdite, sauf consentement préalable des personnes concernées.

La problématique

On ne peut pas savoir au moment de la collecte des données personnelles à quoi elles pourront servir dans quelques mois ou années. Surtout dans un contexte d'évolution technologique permanente et de plus en plus rapide.

Le gestionnaire des données est donc un jour ou l'autre tenté d'utiliser les données en sa possession, pour une finalité autre que celle annoncée initialement. Du reste, on rappelle que s'il n'utilise plus les données, le gestionnaire doit les effacer après une période qui dépend de la finalité de départ. Choix cornélien donc : soit j'efface les données si je reste dans la finalité de départ et que celle-ci a été exécutée, soit je les réutilise pour une nouvelle finalité si je souhaite conserver les données.

Les processus de Big data offrent un parfait exemple de la problématique. Les outils de profilage demandent par définition de se nourrir de très nombreuses observations issues de traitements de données divers et variés. La plupart du temps, ces traitements n'ont pas été mis en œuvre pour permettre un processus de profilage. Cette finalité n'était pas prévue initialement (par exemple, l'inscription et la gestion d'un jeu en ligne sur internet ; l'inscription et l'utilisation un site d'échanges en vue de vendre certains biens etc.). La nouvelle finalité est souvent incompatible avec la première et, selon les lois sur la protection des données personnelles, elle est a priori interdite.

Deux interprétations semblaient s'affronter :

• Soit on considérait que la nouvelle finalité incompatible ne pouvait être poursuivie qu'à la condition de recueillir le consentement de la personne concernant la nouvelle finalité d'utilisation des données. Dans notre exemple, le responsable qui veut se relancer dans son projet Big data, doit réinterroger chaque personne afin d'obtenir son consentement explicite sur la nouvelle finalité d'utilisation.

• Soit on admet y voir un nouveau traitement pouvant être poursuivi comme tel, c'est-à-dire en le soumettant à l'intégralité de la protection légale (information des personnes concernant la nouvelle finalité, nouvelles mesures de sécurité ou de sauvegarde si nécessaires, détermination d'une nouvelle base de licéité qui n'est pas forcément le consentement de la personne mais par exemple un équilibre d'intérêts avec droit d'opposition, nouvelle déclaration auprès de l'autorité de protection des données etc.). Cette deuxième opinion, plus souple, permet d'admettre une évolution inévitable des finalités d'utilisation, tout en garantissant les droits et libertés de la personnes.

Le système sévère du futur Règlement

La disposition finale du projet de Règlement ne comprend plus aucune disposition concernant le problème du changement de finalité et les conditions dans lesquelles il aurait pu intervenir.

L'évolution du texte témoigne d'un véritable débat sur ce point.
Le texte initial ne contenait aucune règle spécifique.

La seconde version a introduit un nouveau paragraphe ayant cet objet (article 6§4). Si les données étaient collectées par le même responsable du traitement, la poursuite d'une finalité ultérieure aurait été permise malgré l'incompatibilité des finalités, pour autant que l'on ait pu justifier celui-ci par une des hypothèses générales de licéité prévue au §1er(consentement, exécution d'un contrat, intérêt vital de la personne etc.).

En d'autres termes, selon la deuxième version du texte, le responsable aurait toujours pu remédier à une incompatibilité entre la finalité initiale et les finalités ultérieures du traitement, en identifiant une nouvelle base de licéité du traitement. En fin de compte, le responsable pouvait toujours prendre le risque de fonder la licéité du nouveau traitement sur la fameuse balance des intérêts, et gérer les soucis a posteriori.

La dernière version du Règlement, ayant fait l'objet du dernier vote en commission, a purement et simplement retiré ce paragraphe.

Le Groupe Article 29 a donc obtenu satisfaction, lui qui avait fortement critiqué cette disposition qui, à ses yeux, mettait à mal et vidait de sa substance le principe de finalité (cfr. Article 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, p. 36 et 37).

Le principe de base est dès lors celui de l'exigence de la compatibilité des finalités nouvelles avec les finalités initiales, sauf consentement de la personne concernée ou un texte légal spécifique le permettant pour des finalités spécifiques (sécurité nationale, défense, sécurité publique etc.) En cas d'incompatibilité, la poursuite de la finalité incompatible est donc prescrite et le changement de finalité rendu illicite.

Des conséquences pratiques importantes

Le Règlement choisit donc la sévérité concernant le régime de changement des finalités.

L'interdiction de traitement en cas d'incompatibilité des finalités s'oppose à l'évolution d'un traitement de données qui est en quelque sorte « figé » par sa finalité réelle de départ. Si des données ont été traitées pour les besoins d'exécution d'un contrat, elles ne pourront la plupart du temps pas être traitées pour une communication à un tiers en vie d'alimenter un processus de profilage big data car ce sera considéré comme finalité incompatible, sauf à obtenir a posteriori le consentement de chacune des personnes concernées.

Sans aller jusqu'à autoriser le changement de finalité sans garantie particulière, un moyen terme était possible si on était parti du principe que la seconde finalité générait un « nouveau » traitement qui devait être soumis au respect de l'intégralité des dispositions de la loi (nouvelle information des personnes, identification d'un nouveau critère de licéité, identification des mesures de sécurité spécifiques, le cas échéant, etc.) et pas seulement à la seule exigence de la licéité.

La solution du Règlement est autre : on ne peut pas modifier une finalité annoncée sans le consentement préalable de la personne. Ce qui pose non seulement problème pour le traitements futurs mais aussi question pour les traitements antérieurs ou qui seront en cours au moment de l'entrée en vigueur du futur Règlement. Le Règlement ne prévoit en effet pas de régime transitoire.

Réagissez à cet article

Source : *Nouveau Règlement vie privée : la réutilisation de données sera-t-elle encore possible ?*

Vol et fuite de données, comment les éviter ?

Vol et fuite de données, comment les éviter ?

Les données, tout le monde le sait désormais, sont d'une importance capitale et d'une valeur inestimable. En tant qu'entreprise, comment les valoriser et surtout comment bien les protéger ?

Et si vous possédiez déjà l'argile des futurs développements de votre entreprise ? En effet, en travaillant les données récoltées par les différents services de votre société, vous pouvez déjà optimiser vos produits et services actuellement commercialisés notamment via l'analyse des données liées à la satisfaction des clients. Mais, plus encore, vous pouvez également faire évoluer vos produits et services voire en créer de nouveaux. **L'étude des data permet de comprendre les usages et de modifier les produits et services en fonction de ces usages**.
Citons les statistiques sur les données révélant les besoins des usagers des transports publics. Citons plus précisément la compréhension des verbatims-clients grâce au logiciel d'analyse sémantique de Dictanova. Citons encore les données issues de l'analyse des cultures agricoles récoltées par les sondes de Weenat.

Déclaration à la CNIL obligatoire

Pour réussir parfaitement cette utilisation, certaines précautions doivent être prises et en tout premier lieu, lorsque votre base de données contient des données personnelles, il est absolument nécessaire de procéder au préalable aux déclarations CNIL (simplifiées, normales voire demande d'autorisation). Outre les potentielles sanctions administratives et pénales, un fichier non déclaré est considéré comme illicite et ne peut donc être ni vendu ni loué. Les juges ont clairement déclaré qu'**un tel fichier non déclaré constituait un objet illicite, hors commerce, insusceptible d'être vendu** (Com. 25 juin 2013). Rappelons également que l'introduction dans un fichier d'une donnée personnelle nécessite le consentement éclairé et préalable de la personne concernée.
Mais, la Data, c'est également une multitude d'informations qui n'ont aucun rapport avec les données personnelles. On peut les appeler « données objectives » ou « données brutes ». Or, au cœur de votre entreprise, il y a aussi de telles informations qui sont certes, plus ou moins organisées. Sachez qu'une fois optimisée en base de données, la data est une véritable mine d'or.

Droit d'auteur ou droit du producteur ?

En organisant vos données, vous valorisez à la fois le contenu (la data) et le contenant (la ou les bases de données). La base de données peut être protégée par le droit d'auteur si le choix ou la disposition des matières constitue une création intellectuelle originale c'est-à-dire lorsque son auteur ou son concepteur fournit un effort personnalisé, éloigné de toute logique automatique et contraignante (cf. article L112-3 du Code de la propriété intellectuelle).
La base de données peut également être protégée via la reconnaissance de la qualité de **producteur de bases de données**. Ici, il s'agit de démontrer en particulier le risque des investissements sur la base de données lors de sa constitution, sa vérification ou sa présentation : investissement financier, matériel ou humain substantiel relevant des moyens consacrés à la recherche de données existantes, à leur rassemblement et le suivi de la base (cf. article L341-1 du Code précité).
Par conséquent, droit d'auteur ou droit du producteur de base de données, vous pouvez être titulaire d'un véritable droit de propriété sur vos données via l'existence de véritables bases de données.
A ce titre, vous pouvez vous en **réserver l'exclusivité** et délivrer à vos clients des prestations de service ou des licences d'utilisation, issues de l'exploitation des données. La seule réserve dégagée par les juges est l'abus de position dominante de telle manière qu'un monopole sur certaines données ne doit pas être préjudiciable aux autres acteurs économiques (Com. 4 décembre 2001 – France Télécom et son fichier d'abonnés).
Sans l'organisation de la data au sein de bases de données, votre data est de libre parcours. Elle relève du bien commun. Titulaire d'un droit de propriété intellectuelle, vous pouvez interdire certaines formes d'extraction et d'utilisation du contenu de votre base et donc de votre data. Dans ces conditions, invoquer un acte de contrefaçon est plus aisé que de démontrer un acte de concurrence déloyale ou de parasitisme.
Parce qu'une fois organisées, les données de votre entreprise ont de la valeur, il faut cultiver votre data, sans trop dénaturer la maxime de Voltaire « Il faut cultiver notre jardin » !

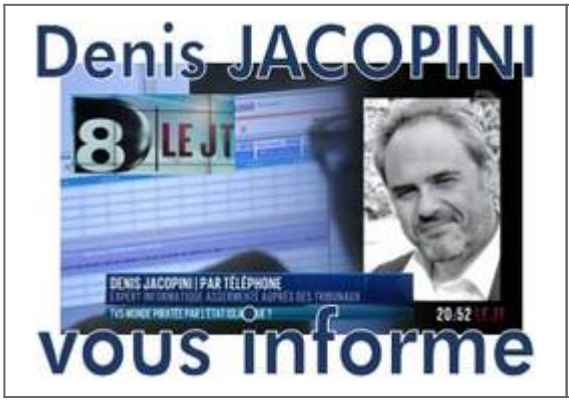
Réagissez à cet article

Source : *Startup : Comment bien protéger sa data, ce précieux patrimoine immatériel ? – Maddyness*

Par Marie-Pierre L'hopitalier, avocat associé.

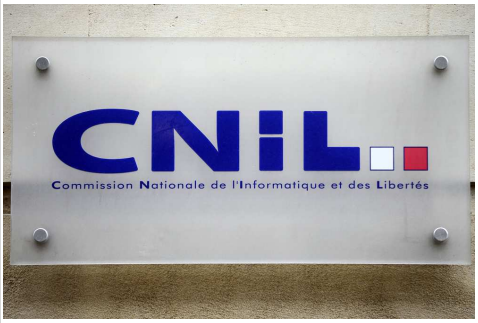
Crédit photo : Shutterstock

La CNIL sanctionne une société marketing



La CNIL sanctionne une société marketing

La Commission Nationale Informatique et Libertés vient de lancer un « avertissement public » à l'encontre de la société marketing Profils Seniors, pour « collecte déloyale » de données personnelles.



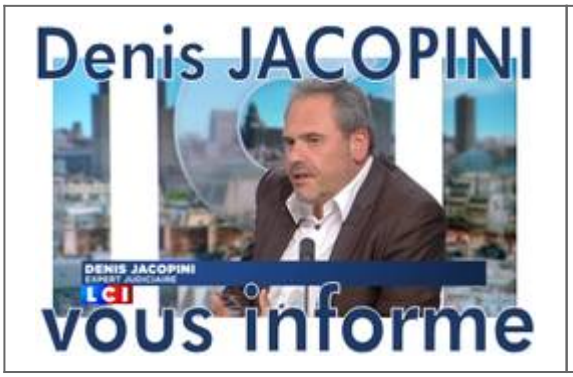
Profils Seniors est une petite société basée dans l'Essonne et « a pour activité la constitution d'une base de données de seniors qu'elle loue à des tiers effectuant de la prospection commerciale électronique », rappelle la CNIL dans son communiqué.
Or, les personnes interrogées par téléphone ne sont pas informées clairement de cette finalité, ce qui amène « à considérer cette collecte comme déloyale », estime l'organisme, chargé de veiller au respect des données personnelles faisant l'objet d'un traitement informatique.
Ainsi, selon les contrôles réalisés sur place par la CNIL en 2015, « les personnes appelées pensent participer à une enquête sur la consommation des ménages français, alors que l'appel vise également à constituer une base de données de seniors qui feront l'objet de prospection commerciale électronique par des tiers ».

Du non-consentement préalable à la non-protection des données personnelles
Par ailleurs, « la société ne recueillait pas le consentement préalable des personnes à recevoir de la prospection commerciale par voie électronique, tel qu'exigé par les textes » et « n'assurait pas la sécurité et la confidentialité des données personnelles qu'elle traitait », ajoute la CNIL.
De plus, Profils Seniors n'assurait pas « la sécurité et la confidentialité des données personnelles qu'elle traitait et qu'il n'existait pas de contrat ou de clauses spécifiques avec ses sous-traitants permettant de leur imposer des conditions de sécurité et de confidentialité des données » et n'avait pas « déposé une demande d'autorisation pour le transfert des données vers des sous-traitants situés dans des pays en dehors de l'Union européenne », souligne la commission.
Les sanctions que peut prononcer la CNIL vont de l'avertissement au retrait d'autorisation, en passant par la sanction pécuniaire (150.000 euros maximum) et l'injonction de cesser le traitement de données concernées.
L'organisme, qui plaide lui-même régulièrement pour un renforcement de ses pouvoirs, souligne par ailleurs que l'adoption du règlement européen sur les données personnelles lui permettrait, à partir de 2018, d'infliger des sanctions allant jusqu'à 4% du chiffre d'affaires de la société incriminée.

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*

Des règles désormais plus strictes pour la protection des données privées



Des règles désormais plus strictes pour la protection des données privées

---

La réforme décidée par le Parlement, la Commission et le Conseil européen aura de profondes implications. De plus le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Après 3 ans, Parlement, Commission et Conseil Européen, le « trilogue » bruxellois, sont d'accord sur la réforme de la protection de la vie privée. La directive de 1995 et ses mises à jour étaient obsolètes et furent transposés sans harmonie dans les Etats, d'où l'idée d'un règlement qui s'appliquera tout de suite.

Ce règlement s'applique aux données privées traitées, pas celle qui sont stockées en vrac. Ce sont les résultats qu'on tire de l'exploitation de ces données qui sont dangereuses. Le règlement ne s'appliquera pas aux traitements des données dans un cadre privé (ouf !). Les autorités judiciaires ne seront pas soumises au contrôle des commissions de vie privée

Celui qui gère et traite vos données (le data controller) devra bien être identifié et réel. Celui qui héberge ses données (data processor) tombe aussi sous le règlement : s'il n'est pas établi dans l'Union, le règlement s'applique à lui quand même , surtout s'il s'agit de profiler le comportement en ligne des citoyens européens. Le pays superviseur sera celui du pays du siège principal du data controller et non pas là où les data centers ont été (dé)localisés. C'est à ce prix qu'un Amazon ou Google n'aura plus à dépendre de 28 commissions de vie privée différentes. Si l'entité n'est pas présente dans l'Union, elle doit mandater un représentant.
Le règlement évoque la pseudonymisation, une contraction d'anonymisation et pseudonyme : l'usage de pseudonymes n'exempte pas les sites d'appliquer le règlement, car on peut souvent remonter à qui est derrière. Par contre, le règlement ne s'applique plus après un décès !

Consentement
Le consentement de l'individu au traitement de ses données, qui existe depuis 1995, sera explicite et non tacite). Le data controller doit en garder la preuve: elle sera non valable si l'utilisateur final a subi un petit chantage (par ex. un service dégradé sans ces données privées). Pour la recherche scientifique, on admet qu'il n'est pas facile de demander à l'avance ce consentement, car on ne sait pas toujours ce qui va en sortir.
Si le data controller détecte des crimes ou des menaces à l'ordre public, il doit les communiquer aux autorités. Idem en cas de cybermenace.
Si le traitement des données vise un but humanitaire, de santé publique (épidémies), ou un cas d'urgence pour l'utilisateur final, leur traitement va de soi, consentement ou pas!
Les données sur l'emploi, la protection sociale et les revenus devraient aussi pouvoir être exploitées si le but est, pour l'État, d'augmenter le bien-être public et une politique ad hoc.
Le traitement de données personnelles doit être proportionnel : si on peut l'éviter à service équivalent, c'est mieux. De même, si la société qui a des données de vous ne sait pas vous identifier, elle ne doit pas chercher à le savoir pour… avoir votre consentement.

Les données sensibles : race, religion, opinion politique
Les données liées à l'exercice de droits et de choix fondamentaux, comme la religion, l'appartenance politique ou la race bénéficient d'une protection renforcée. Leur traitement devrait être une exception et soumis, avant leur exécution, à une analyse d'impact du risque encouru d'un tel profilage. Par contre, les photographies ne seront pas protégées saut à contenir des données biométriques.

Accès et rectification de données chez les tiers
Le droit à la rectification doit être aisé à exercer, en ligne par exemple si les données ont été collectées ainsi. Une réponse, oui ou non, sera fournie dans le mois.
À charge pour le data controller de vérifier que celui qui adresse sa demande d'accès est la bonne personne. Le droit à l'oubli à la «Google» devient… un droit à l'effacement si les données collectées ne sont plus nécessaires ou ne sont plus traitées. Ce droit à l'effacement s'opérera en cascade : les entités qui auraient rendu les données publiques seront obligées d'informer les autres qui les exploiteraient ou les auraient copiés.
À une demande d'une copie de ses données personnelles (droit d'accès), c'est un format lisible par un humain qui est exigé, pas du binaire ! D'ailleurs, dit le règlement, ne faudrait-il pas un format de donnes interopérables pour permettre, enfin, la portabilité des données entre sociétés. Il n'est pas précisé si c'est applicable au cloud (car c'est du stockage, pas du traitement). Le règlement évoque les algorithmes qui prennent des décisions sur base des données personnelles ainsi que le profilage.

Fuites et vol des données
Les fuites de données devront être notifiées aux autorités et aux personnes impactées dans les 72 heures à moins que leur chiffrage ne les rendent inviolables. À noter tout de même un relâchement de l'obligation de notifier à la commission de vie privée tous les traitements des données personnelles, uniquement les cas risqués d'atteintes aux droits et libertés fondamentales.

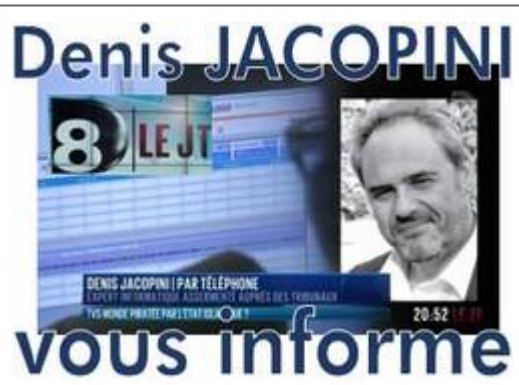
Échanges internationaux
Les données peuvent être échangées avec des pays tiers en dehors de l'Union : c'est à la Commission de statuer si le pays répond ou non aux exigences minimales de sécurité. La Commission peut aussi retirer son agrément.
Le data controller peut toutefois continuer à opérer avec un pays « peu sûr » s'il compense avec des mesures de sécurité supplémentaires. Les sociétés peuvent mettre en place entre leurs filiales des règles internes pour atteindre un même niveau de sécurité que le règlement. Attention aux échanges avec des pays tiers (ex : les USA à la demande d'une cour) et donc à l'application extraterritoriale de ses lois à des citoyens européens : ils sont autorisés s'ils sont couverts par un traité d'assistance mutuel.
Le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Réagissez à cet article

Source : *Serrage de vis européen sur la protection des données privées – Le Temps*

Infractions aux données

personnelles : les associations pourraient se porter partie civile – Politique – Numerama

	Infractions aux données personnelles : les associations pourraient se porter partie civile – Politique – Numerama

Les députés ont ajouté dans le projet de loi Lemaire la possibilité pour certaines associations de se porter partie civile lorsque le parquet poursuit des infractions pénales liées à la protection des données personnelles.

Le gouvernement estimant urgent d'attendre l'adoption du règlement européen sur les données personnelles, qui ne laissera selon Axelle Lemaire « *aucune marge de manœuvre* » aux États, les députés ont rejeté jeudi un amendement qui aurait permis de muscler très sensiblement les sanctions que peut prononcer la CNIL lors d'infractions à la législation sur la protection des données personnelles. Il aurait mis fin à ces situations ridicules qui font que Google, pris la main dans une confiture très grasse, ne se voit infliger qu'une amende équivalente à 2 minutes de chiffre d'affaires.
Mais en attendant, les députés ont tout de même fait ajouter au projet de loi d'Axelle Lemaire une disposition qui autoriserait les associations à se porter civile, et donc à réclamer des dommages et intérêts, lorsque des individus ou des entreprises commettent des infractions pénales liées aux données personnelles.

Des dommages et intérêts

Le texte dispose en effet que « *toute association régulièrement déclarée depuis au moins deux ans à la date des faits, se proposant, par ses statuts, de protéger les données personnelles ou la vie privée peut exercer les droits reconnus à la partie civile en ce qui concerne les infractions prévues aux articles 226-16 à 226-24 du code pénal* », réunies sous le titre des « *atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* ».
Parmi ces dernières figure notamment l'irrespect des préconisations légales imposées par la loi CNIL, le défaut de sécurisation dans les traitements de données personnelles, la conservation hors délai des données, la constitution sans autorisation de certains fichiers de données sensibles, ou encore l'obtention de données par fraude.
L'amendement adopté précise que « *quand l'infraction aura été commise envers des personnes considérées individuellement, l'association ne sera recevable dans son action que si elle justifie avoir reçu l'accord de ces personnes* »… Lire la suite

---

Réagissez à cet article

Source : *Infractions aux données personnelles : les associations pourraient se porter partie civile – Politique – Numerama*

Auteur : Guillaume Champeau

Propriété des données personnelles dans la loi Lemaire

	Propriété des données personnelles dans la loi Lemaire

L'article 26 de la loi Lemaire inscrit le droit à la libre disposition de ses données personnelles dans la loi du 6 janvier 1978 dite « informatique et libertés ». Bien que s'en défendant explicitement dans son exposé des motifs, la loi pour une République numérique introduit en droit français la propriété des données personnelles. Pour le meilleur et, surtout, pour le pire.

L'article 26 de la loi pour une République numérique consacre la libre disposition des données personnelles, ce qui recouvre « le droit à la libre disposition de ses données, c'est-à-dire le droit de l'individu de décider de contrôler l'usage qui est fait de ses données à caractère personnel ». Cela revient ni plus ni moins qu'à reconnaître un droit de propriété sur ses données personnelles. Pourquoi ? Parce que vient d'être consacré le dernier des trois éléments du droit de propriété sur les données personnelles, qui ne l'était pas encore.

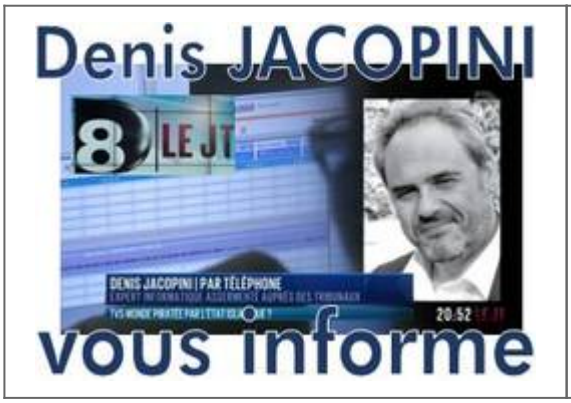
En effet, l'article 544 du Code civil définit la propriété comme « le droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements ». Les juristes ont, de longue date, distingué trois composantes de ce droit de propriété : l'usus – la faculté d'usage –, le fructus – le droit de percevoir les fruits de sa propriété – et l'abusus – le droit de disposer, incluant celui de mettre fin à sa propriété. À titre d'exemple, le propriétaire d'un appartement peut donc l'utiliser pour soit en l'habitant (usus), en tirer les revenus qu'il peut engendrer de par sa mise en location (fructus) ou tout simplement le vendre (abusus).
Et les données personnelles ? Avant l'article 26 précité, chaque personne en était simplement usufruitière. La loi ne lui reconnaissait tacitement que l'usus et le fructus, proscrivant tout aussi tacitement l'abusus. Une personne pouvait ainsi utiliser ses données personnelles (par exemple fournir ses coordonnées pour la réalisation d'un contrat et/ou d'une prestation de service) et en retirer les fruits (obtenir un compte mail en apparence gratuit en échange de la « location » de ses données personnelles). Elle ne pouvait toutefois pas s'en séparer, par exemple en les vendant.
La raison d'une telle limitation réside dans l'existence d'un principe structurant au sein de la loi dite « informatique et libertés » : celui de finalité. Il subordonne l'emploi de tout usage non strictement intime de données personnelles à l'existence d'une finalité considérée comme légitime par le législateur. À défaut de quoi, le traitement est illicite. C'est ce qui lui permet d'assurer les équilibres voulus par le législateur, à savoir concilier l'usage le plus étendu possible de l'informatique avec la protection de valeurs nécessaires à la vie en société.

Au premier rang desquels les droits et libertés fondamentales de la personne humaine, y incluant la protection de sa liberté et de sa vie privée. Sans leur respect effectif, nous ne sommes plus dans une démocratie libérale – qui implique une liberté effective de choisir ses gouvernants, donc l'existence d'une sphère privée pour nourrir et étayer cette liberté –, mais dans un régime à la 1984 de George Orwell. La question de la protection des données personnelles, à rebours d'une conception traditionnellement individualiste, est donc éminemment politique.
Il est donc formellement vrai que la loi Lemaire ne consacre pas le droit de propriété sur ses données personnelles étant donné qu'il existait avant cela une patrimonialité limitée à l'usus et au fructus. L'article 26 de cette loi se contente, de manière en apparence anodine, de consacrer sur les données personnelles le seul élément du droit de propriété qui ne leur était pas encore reconnu : l'abusus. Or, la libre disposition des données personnelles entre en contradiction avec le principe de finalité. En effet, disposer de ses données signifie pouvoir en perdre de vue l'utilisation, qui peut alors être réalisée pour une finalité ultérieure non déterminable au moment du transfert.
C'est là qu'est le cadeau empoisonné : le pouvoir de contrôle défini par l'article 26 de cette loi n'est qu'une faculté reconnue à la personne fichée, faculté qui vient se substituer au contrôle obligatoire de la CNIL. Or, il existe un décalage considérable entre l'innocuité apparente d'un transfert de données personnelles et la technicité extrême de l'encadrement de cette question par le droit. Pour donner un ordre d'idée, le dernier projet de règlement européen en la matière, qui devrait être adopté au printemps 2016, fait dans sa dernière version 209 pages. Est-il réaliste de croire que chaque personne fichée maîtrise sur le bout des doigts chacune de ces pages ?
Remplacer le contrôle obligatoire de la CNIL par le contrôle facultatif de tout un chacun, non spécialiste du droit des données personnelles, apparaît donc comme séduisant de prime abord. Mais cela n'aboutit qu'à donner à toute personne fichée les clefs d'une servitude accrue, en lui permettant d'entériner, par son consentement, le contournement des équilibres autrefois obligatoires de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La libre disposition des données personnelles rend possible la propriété des données personnelles et ouvre la voie à une servitude accrue de la personne fichée. Merci Mme Lemaire.

Réagissez à cet article

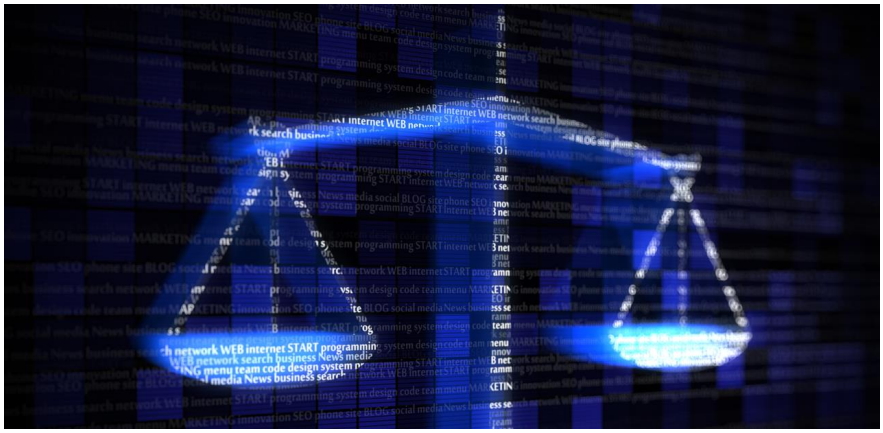
Source : *La propriété des données personnelles : ce cadeau empoisonné de la loi Lemaire, Le Cercle*

Retard pour la plateforme nationale des interceptions judiciaires



Retard pour la plateforme nationale des interceptions judiciaires

plateforme nationale des interceptions judiciaires (PNIJ) a du plomb dans l'aile. Pour remédier au retard de son déploiement, le gouvernement a décidé de reporter l'abrogation du STIJ, le système de transmission des informations judiciaires qu'elle doit remplacer.



Créé par un décret du 30 juillet 2007, le fichier STIJ permet « *aux magistrats et aux officiers de police judiciaire de disposer des données de trafic des correspondances interceptées (numéros de téléphone, date, heure et durée de l'appel, etc.) ainsi que des contenus des messages (SMS, MMS) émis ou reçus par un numéro de téléphone dont la ligne est surveillée* » , résumait la CNIL en 2014.

Ce dispositif n'était que temporaire. Il devait être remplacé par la plateforme nationale des interceptions judiciaires six mois après l'entrée en vigueur de celle-ci et au plus tard au 31 décembre 2015. La PNIJ a en effet pour mission de centraliser le recueil des données de connexion et des interceptions de correspondances décidés par un juge. Elle tranche avec les pratiques jusqu'alors en vigueur « *où les dispositifs d'interception des communications électroniques et les réquisitions de données de connexion reposaient sur un système hétérogène et décentralisé* » dixit la CNIL.

Report d'un an

Seulement, il faut croire que le passage de relais ne se passe pas aussi bien que prévu. Hier, au Journal officiel, le gouvernement a en effet décidé de reporter l'abrogation du STIJ au 31 décembre 2016. Pour comprendre pourquoi, il faut lire la délibération de la CNIL publiée à cette occasion.

Selon la Commission, la version actuelle de la PNIJ « *ne permet pas techniquement de traiter les données prévues à l'article R. 40-46-2° du Code de procédure pénale* », c'est-à-dire les données faisant l'objet d'une mesure de géolocalisation en temps réel. Autre fonctionnalité en souffrance, dont la Commission révèle l'existence : « *la fonction de reconnaissance vocale du locuteur n'est pas disponible* ». Bref, de nouveaux développements sont nécessaires pour parfaire ce chantier, des travaux qui prendront plusieurs mois.

Un passage de relais délicat

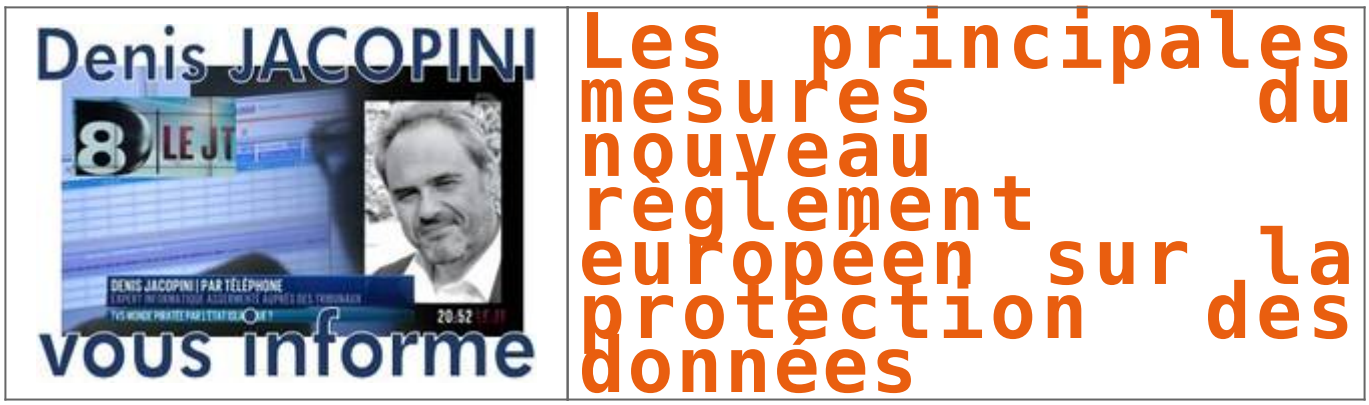
Le basculement du STIJ à la PNIJ devra aussi être l'occasion d'un gros ménage puisque la CNIL a interdit que les données de l'un soient reprises par l'autre. Il faudra donc organiser un effacement, en tenant compte des différentes durées de conservation. Un exercice rendu d'autant plus complexe par l'éparpillement des informations sur les postes de travail des enquêteurs.

Rappelons que la plateforme nationale des interceptions judiciaires, située dans les locaux du géant Thales, est placée sous le contrôle d'une personnalité qualifiée (article R40-53 du Code de procédure pénale). C'est Mireille Imbert-Quaretta, l'ancienne présidente de la commission de protection des droits à la Hadopi, qui occupe désormais ce poste pour une durée de cinq ans. Elle devra établir un rapport annuel qu'elle adressera au garde des sceaux, ministre de la justice. Sur cette question, la CNIL a déploré ne pas être destinataire de ce rapport, mais le ministère de la justice lui a promis de lui en adresser un exemplaire.

Réagissez à cet article

Source : *Du retard pour la plateforme nationale des interceptions judiciaires – Next INpact*

Les principales mesures du nouveau règlement européen sur la protection des données



L'UE a approuvé le 15 décembre au soir le règlement sur la protection des données, qui renforce considérablement les pouvoirs de sanction des Cnil nationales.
La Commission européenne, le Parlement européen et le Conseil européen, qui travaillent depuis cet été à la constitution d'un compromis, se sont entendus le 15 décembre au soir sur un règlement européen sur la protection des données, qui harmonise des législations nationales très variées (voire inexistantes) pour donner aux citoyens un meilleur contrôle sur la façon dont leurs données sont collectées et utilisées. Comme tout règlement, celui-ci n'aura pas besoin d'être transposé en droit national et s'appliquera directement à partir du début 2017.

Parmi les principales mesures approuvées, on trouve :
Un important pouvoir de sanction accordé aux différentes « Cnil » nationales, qui pourront infliger des amendes allant jusqu'à 4% du chiffre d'affaires mondial (jusqu'à un certain plafond) des entreprises qui utilisent à mauvais escient les données numériques des gens, notamment en y accédant sans leur consentement. Autrement dit, des amendes pouvant atteindre plusieurs millions d'euros qui devraient a minima constituer une bonne dissuasion. Toutefois, pour ne pas empêcher les entreprises de tirer profit du big data, elles pourront traiter librement les données une fois effacée l'identité précise des utilisateurs.
L'obligation, pour les entreprises victimes de fuite de données, de signaler leur cas aux régulateurs nationaux sous trois jours, sous peine là encore de fortes amendes.
Le droit à l'oubli, entériné par le règlement, qui permet aux citoyens européens de demander à supprimer des informations en ligne qui les concernent mais ne sont plus pertinentes.
La portabilité des données, qui permet aux utilisateurs de demander le transfert de leurs données d'une plateforme vers une autre.
L'obligation, pour les moins de 16 ans, de demander une autorisation parentale avant de pouvoir utiliser des services tels que Facebook, Snapchat ou Instagram. Bruxelles proposait 13 ans comme aux Etats-Unis, mais certains pays dont la France ont poussé pour relever cette majorité numérique. Chaque Etat membre est toutefois libre d'y déroger.

L'extension de ces nouvelles règles à toutes les sociétés qui comptent des utilisateurs dans l'Union européenne, même si elles sont basées hors de l'UE. Dans la Silicon Valley par exemple.
Autrement dit, le règlement se fait beaucoup plus protecteur des citoyens européens que la législation équivalente aux Etats-Unis, mais également bien plus sévère à l'égard des sociétés qui y contreviendraient.
Naturellement, les géants américains ont protesté en accusant l'Union de les cibler injustement, au détriment de leurs petits rivaux européens. Ils estiment en particulier que lier les sanctions au chiffre d'affaires mondial n'a pas de sens. Mais l'UE, qui a toujours rejeté ces accusations, est restée ferme. Les grandes plateformes US ont donc sans doute du souci à se faire, à l'instar d'un Facebook qui a déjà eu maille à partir avec les régulateurs nationaux en France, en Espagne, en Allemagne, aux Pays-Bas et encore récemment en Belgique.

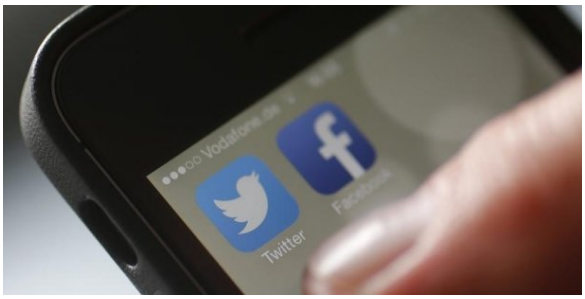
Réagissez à cet article

Source : *Les principales mesures du nouveau règlement européen sur la protection des données | CHABERT CATHERINE*

L’UE parvient à un accord de principe sur la protection des données personnelles

L’UE parvient à un accord de principe sur la protection des données personnelles

Les États membres conservent toutefois à leur charge la question de déterminer l'âge minimum requis pour les mineurs sur les réseaux sociaux.



Après quatre ans d'âpres discussions, un accord de principe a finalement été trouvé mardi 15 décembre à Bruxelles, afin d'adapter la législation européenne sur la question de la protection des données personnelles à l'heure d'internet. Le texte a été validé à l'occasion d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.

« L'UE aura désormais la législation la plus étendue de protection des données personnelles dans le monde », s'est réjouie l'eurodéputée Sophie in 't Veld (libérale). L'accord prend en compte la décision récente de la justice européenne qui a déclaré « invalide » le cadre juridique qui couvre le transfert par Facebook de données personnelles de l'UE vers les Etats-Unis, a-t-elle souligné.

Des entreprises inquiètes des sanctions

L'accord tente de faire la synthèse entre l'exigence de donner plus de moyens de contrôle aux citoyens quant à leurs informations personnelles et la nécessité d'harmoniser les législations des États membres afin de faciliter le travail des entreprises.

Parmi les autres points de discussion, figurait notamment le montant des amendes que devront payer les entreprises qui violent les règles européennes sur la protection des données. Au terme de l'accord, les géants d'internet pourraient se voir sanctionner à hauteur de 4% de leur chiffre d'affaires annuel mondial.

Quel âge minimum sur les réseaux sociaux?

Selon cet accord, les États membres pourront fixer librement « entre 13 et 16 ans » l'âge auquel un mineur peut s'inscrire sur des réseaux sociaux comme Facebook ou Snapchat, sans l'accord d'un parent, a indiqué l'Allemand Jan-Philipp Albrecht (Verts), rapporteur du Parlement européen sur la réglementation de la protection des données.

« Malheureusement, les États membres n'ont pas pu se mettre d'accord pour fixer une limite d'âge à 13 ans pour le consentement parental à l'utilisation de réseaux sociaux comme Facebook ou Instagram », a expliqué Jan-Philipp Albrecht, à l'issue d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.

Le Parlement européen voulait fixer cette limite à 13 ans, soit l'âge minimum requis indiqué par Facebook, mais certains Etats membres s'y sont opposés.

Un accord contraignant

L'accord devra encore être confirmé par le Conseil européen et voté par le Parlement au début de l'année 2016. Il restera ensuite deux ans aux États membres pour le faire entrer en vigueur. L'accord, qui comprend un règlement et une directive, a vocation à s'imposer à tous les États membres.

En juin, les ministres européens de la Justice avaient déjà trouvé un accord sur la création d'un « guichet unique » compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entreprises ou des plateformes internet comme Amazon, Google et Facebook.

Réagissez à cet article

Source : *Protection des données personnelles: l'UE parvient à un accord de principe*