# 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

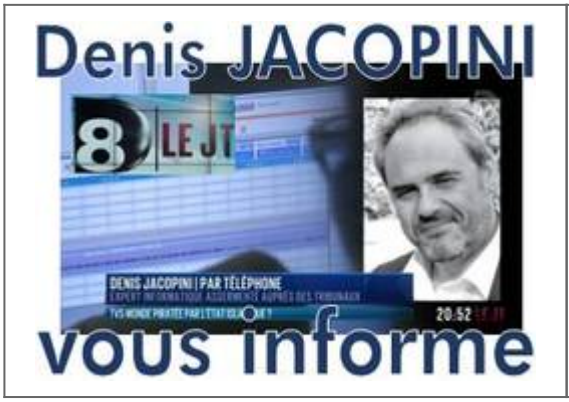
Source : *Startup : Comment bien protéger sa data, ce précieux patrimoine immatériel ? – Maddyness*

Par Marie-Pierre L'hopitalier,  avocat associé.

Crédit photo : Shutterstock

---

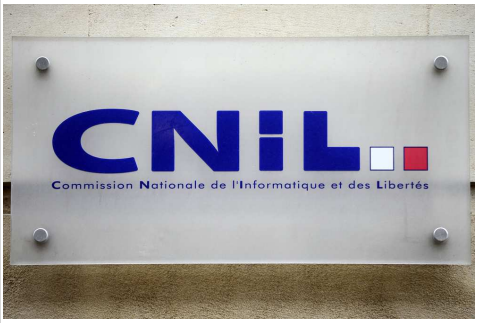
# La CNIL sanctionne une société marketing




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.*

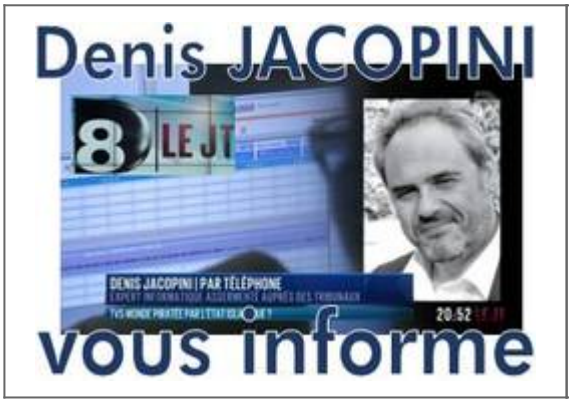
---

*Réagissez à cet article*

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

---

# Vos données personnelles en otage, puis chantage




Vos données personnelles en otage, puis chantage

---

**Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité**

**Quel mode opératoire ?**

Le mode opératoire est toujours sensiblement le même :
Un individu parvient à s'introduire dans le système informatique d'une entreprise ou d'un particulier. en extrayant les données y étant stockées.
Dans un second temps, l'internaute ou l'entreprise victime se voit réclamer le versement d'une rançon.
A défaut de paiement, ces informations personnelles seront diffusées sur la toile.
L'exemple le plus significatif en la matière est le cas du site de rencontres extraconjugales canadien ASHLEY-MADISON.COM, victime d'une cyberattaque le 15 juillet 2015.
Un groupe de « hackers » se faisant appel « The Impact Team » a réussi à pénétrer sur les serveurs du site et à en récupérer les données relatives à ses 37 millions d'abonnés de par le monde.
La fermeture du site a alors été exigée, son éditeur se voyant menacé d'une publication en ligne de l'intégralité de ses données. Précisons que cette menace a été mise à exécution au cours du mois d'août 2015.
Une fois ces informations rendues publiques, certains (anciens) clients du site se sont vus demander la remise de fonds, à défaut de quoi leurs informations personnelles seraient adressées directement à leurs proches ou à leurs relations professionnelles.
Autant dire que l'image de l'entreprise victime est ternie, la sécurité de son système informatique étant clairement remise en cause.
Les abonnés voient également des informations (très) personnelles dévoilées publiquement, telles que leur lieu de résidence, leurs coordonnées bancaires, leurs loisirs et habitudes de consommation, leurs fantasmes et désirs sexuels.

**Dans une moindre mesure, les particuliers peuvent être individuellement les cibles de phénomènes de ce type.**

Pour ces derniers, il prendra la forme d'un programme informatique malveillant appelé « rançongiciel », dérivé de l'anglicisme «ransomware » et, précisons-le, contraction des termes « rançon » et « logiciel ».
Ce programme chiffre ou crypte les données de l'internaute, présentes sur le disque dur de son ordinateur.
Si il souhaite les récupérer ou éviter leur divulgation, il devra là encore payer la rançon exigée.
Une variante consiste à arborer le logo d'une unité de police de type INTERPOL, en accusant l'internaute de détenir illicitement des œuvres protégées par le droit d'auteur ou bien des vidéos ou photographies pédopornographiques.

**Quelles Infractions pénales ?**

**Le chantage et l'extorsion**

« Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. » (article 312-10 du Code pénal)
Ce délit est puni de 5 ans d'emprisonnement et de 75.000,00 Euros d'amende.
« Lorsque l'auteur du chantage a mis sa menace à exécution, la peine est portée à sept ans d'emprisonnement et à 100.000 euros d'amende. » (article 312-11 du Code pénal)
La menace sera mise à exécution, à partir du moment où les données sensibles seront publiées en ligne ou communiquées à des tierces personnes.
« L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. »
« L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende. » (article 312-1 du Code pénal)
En la matière, la contrainte ne reposera pas sur la force physique, mais sera purement morale ou psychologique.

**L'intrusion dans un système informatique**

**L'accès et le maintien frauduleux dans un système**

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. » (article 323-1 du Code pénal)

**L'entrave au fonctionnement d'un système**

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-2 du Code pénal)
Le chiffrement ou le cryptage de données entrave nécessairement le bon fonctionnement d'un sytème informatique.

**La suppression ou la modification frauduleuse de données**

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-3 du Code pénal)

**Les atteintes à la vie privée**

« Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.» (article 226-1 du Code pénal)
« Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l' article 226-1.» (article 226-2 du Code pénal)
L'atteinte à l'intimité de la vie privée sera ainsi caractérisée, lorsque l'objet du chantage consistera en des photographies ou des vidéos représentant des personnes dans un lieu privé.

**La violation du secret des correspondances (électroniques)**

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. » (article 226-15 du Code pénal)
Le délit de violation du secret des correspondances est pleinement constitué, dès lors que la menace porte sur la teneur de courriers électroniques, d'emails ou de messages privés échangés entre abonnés ou utilisateurs d'un site.

**Les infractions à la législation sur les données personnelles**

Le traitement illicite de données personnelles
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »(article 226-16 du Code pénal)
La collecte frauduleuse de données personnelles
« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226–18 du Code pénal)
Le défaut de sécurité des données
La particularité de cette dernière infraction est qu'elle vise, non pas l'auteur de l'attaque, mais bel et bien sa victime directe, le responsable du traitement des données.

En effet, les personnes, entreprises, organismes et collectivités, en charge du traitement des données de leurs utilisateurs ou de leurs usagers, sont tenus de mettre en œuvre toutes les mesures nécessaires, afin d'assurer la sécurité et la confidentialité desdites données.
A défaut, ils engageront leur responsabilité civile et pénale sur le fondement des articles 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 226–15 du Code pénal:
« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » (article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226-15 du Code pénal)

Au cas par cas, d'autres infractions peuvent également être constituées, telles que les délits d'escroquerie, d'usurpation d'identité (numérique), voire même d'usurpation de fonctions, dans la situation où le cyber-délinquant se fait passer pour une unité de police, afin de se faire remettre des fonds.

**Quelles solutions ?**

**La plainte pénale**

Que l'on soit une entreprise, une collectivité ou un particulier victime de ce type d'agissements, le premier réflexe est de déposer plainte auprès des services de police ou de gendarmerie ou bien directement auprès du Procureur de la République.
Ce dernier se réservera le droit d'engager des poursuites ou bien de procéder à un classement sans suite de la plainte, faute notamment de disposer d'éléments suffisants afin d'identifier et de localiser précisément le ou les auteur(s) des faits.
En cas de classement sans suite, la victime disposera alors de la faculté de se constituer partie civile auprès du doyen des juges d'instruction, ce qui déclenchera automatiquement des poursuites pénales.

**Le retrait de contenus illicites**

Si les informations personnelles sont publiées sur un site internet en particulier, leur retrait peut être demandé directement auprès de son éditeur.
A défaut de réponse de sa part ou si il n'existe aucun moyen de le contacter, la suppression des contenus illégaux devra être alors demandée à l'hébergeur du site, en application de l'article 6-I-5 de la loi n°2004-575 pour la confiance dans l'économie numérique.

**Le déréférencement et la désindexation des moteurs de recherche**

Lorsque le nom et le prénom d'une personne sont tapés sur un moteur de recherche, la liste des résultats de recherche peut faire apparaître des liens renvoyant vers les informations frauduleusement obtenues et divulguées.
Dans ce cas, il est envisageable de demander la désindexation de ces liens directement auprès du moteur de recherche et, le cas échéant, par voie judiciaire.

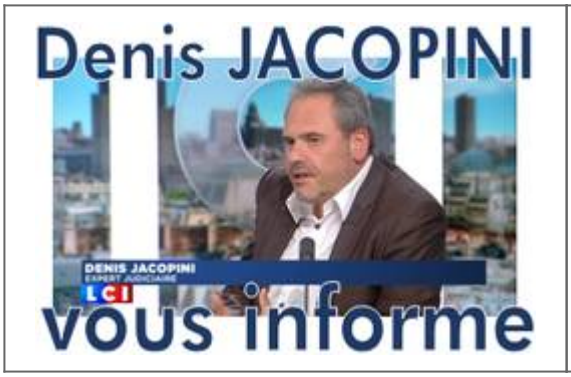
---

Réagissez à cet article

Source : *Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité – Maître thibault prin*
*Thibault PRIN AVOCAT*
*Avocat inscrit au Barreau de PARIS*

---

# 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 ?

---

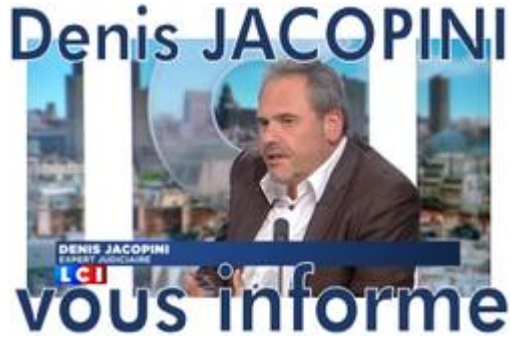
Réagissez à cet article

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

---

# Impact sur les entreprises du

# règlement général sur la protection des données




## Impact sur les entreprises du règlement général sur la protection des données

**Dans un autre article, j'ai insisté sur le fait que l'impact du Règlement général sur la protection des données était lourdement sous-estimé. Dans cet article, j'explique pourquoi la conformité est essentielle, et je passe en revue les étapes à suivre pour s'assurer de la conformité au Règlement. Il ne s'agit pas d'une liste de tâches à accomplir, mais d'un virage fondamental dans la mise en place de la conformité.**

Pour commencer, il existe de nombreuses définitions de la conformité, mais deux principes clés se dégagent :

Le permis d'exploitation : si votre organisation est une banque, un hôpital ou un service public en particulier, sa mission est de se conformer au respect de la vie privée, surtout si elle manipule des données sensibles sur les citoyens. Ce genre d'organisations est toujours exposé à des lois. Il est donc important d'intégrer les processus sans délai, au quotidien ; il ne peut pas s'agir d'un exercice qu'on effectue une fois par an.

Le comportement et la culture de l'organisation : la conformité doit faire partie de l'ADN de toute l'entreprise, et être le catalyseur d'un changement du comportement des employés, même si les initiatives liées à la conformité émanent du Comité de Direction. Si la Direction est la seule à imposer les changements, les appels à la conformité porteront leurs fruits trois ou quatre fois, mais le processus peut se déliter à la cinquième fois.

Étant donné le caractère vital de la conformité, il est important de ne pas prendre en compte les seuls processus technologiques, mais aussi leur intégration aux processus business et à la mise à disposition d'informations. Voici quelques conseils de base pour aider les organisations à appliquer le futur Règlement général sur la protection des données.

**Comprendre la gouvernance des données.**

Avant de s'engager dans un projet de conformité, il est important d'avoir des données de qualité, de comprendre leur origine, le système ou l'application où elles sont stockées, et si les informations sont exactes et complètes. Si des tiers sont impliqués, assurez-vous de l'existence d'accords contractuels relatifs à la conservation et à la propriété de ces données.

Faire une analyse des écarts. Les organisations ont généralement déjà mis en place des contrôles concernant la vie privée. Cependant, lorsqu'un nouvel élément législatif tel que le règlement général sur la protection des données entre en vigueur, il est important de déterminer quels contrôles seront suffisants pour appliquer la législation et d'examiner quels points de contrôles doivent être étendus.

Concevoir et développer des contrôles. Après avoir identifié les faiblesses de votre processus de conformité, par exemple au niveau des ressources humaines ou des finances, il vous faudra définir et mettre en place de nouveaux contrôles pour pallier ces manques.

Installer des logiciels de chiffrement. Afin de garantir le transfert sécurisé des données individuelles, qu'elles concernent un client, un fournisseur ou un employé. Il existe toujours un risque potentiel lié à la vie privée, si ces données sont utilisées à des fins non autorisées.

Prouver la conformité et la traçabilité des informations. Il est important que toutes les données soient en place pour répondre aux questions des auditeurs. Il est envisageable d'avoir recours à un tiers pour exercer une fonction d'assurance qualité avant l'arrivée des auditeurs. Nous aidons les entreprises internationales à faire la preuve de leur conformité, informations précises et exhaustives à l'appui.

De plus en plus, le respect de la vie privée devient une préoccupation. Les organisations doivent avoir une vision complète des données en leur possession, de manière à apporter la preuve solide de leur conformité et à établir une relation de confiance avec les fournisseurs, les clients et les citoyens. Le Règlement général sur la protection des données entrera bientôt en vigueur. Il est désormais temps d'évaluer la gouvernance de vos données et les pratiques de sécurité et de confidentialité qui leur sont appliquées.

---

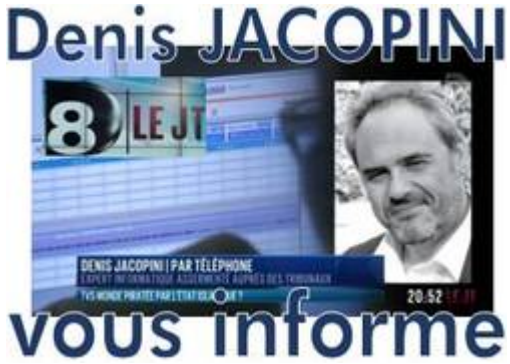
Réagissez à cet article

Source : *Appliquer le Règlement général sur la protection des données – Abbas Shahim, Atos Consulting*

---

# 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.

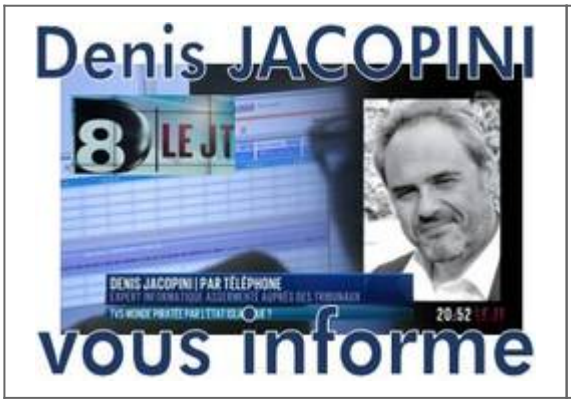
---

Réagissez à cet article

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

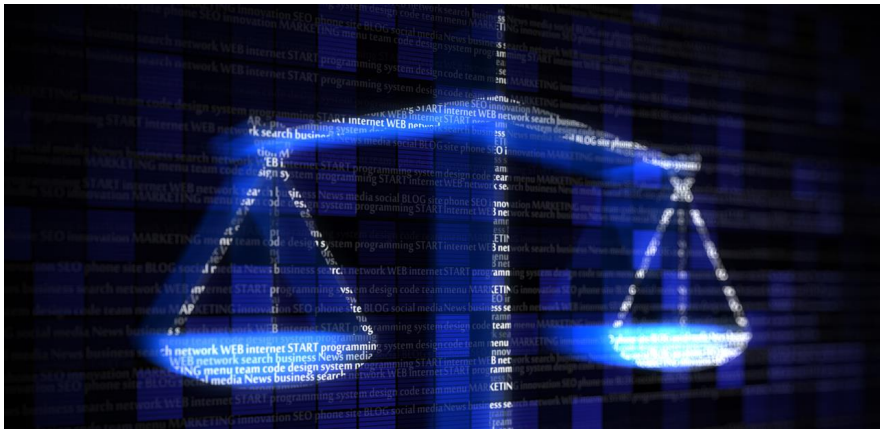
---

# 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*

---

# AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016


AVG dévoile ses prévisions d’attaques informatiques et technologiques pour 2016

---

**L'apparition de voitures autonomes n'est pas le seul élément prouvant que les systèmes logiciels « intelligents » vont améliorer notre sécurité. D'autres indicateurs sont également visibles sur Internet.**
Chez AVG, il nous a fallu des années pour concevoir nos récents algorithmes de détection des brèches et de réputation des fichiers. Pour notre tout dernier moteur antivirus, nous avons utilisé des techniques sophistiquées d'apprentissage neuronal et de collecte de données dans le cloud, qui ont été conçues pour intercepter les logiciels malveillants plus en amont, et de manière plus systématique.

**En 2016, de nouvelles solutions de sécurité fondées sur l'intelligence artificielle vont faire leur apparition.**
On peut donc espérer que la bataille engagée contre les mauvais génies d'Internet va connaître un regain d'énergie très attendu, et que les menaces seront encore plus vite contrées et éliminées. Les progrès de l'intelligence artificielle et des systèmes d'apprentissage profond (ou « deep learning ») sont devenus bien plus accessibles. C'est ce que l'on a pu voir récemment, par exemple, lorsque Google a ouvert le code source de l'outil Tensorflow mis au point au sein de la division chargée de l'intelligence artificielle chez Google.

**Autorités de certification : une disparition annoncée**
La nécessité de sécuriser tout le trafic HTTPS des sites Web via un mode de chiffrement prend de l'ampleur. En 2016, avec l'apparition de nouvelles normes ouvertes et le fait que les propriétaires de sites pourront plus facilement faire des choix, il se pourrait que cette réalité devienne globale. Certaines autorités de certification, qui par comparaison commencent à paraître un peu dépassées, risquent de connaître des moments difficiles.
Ces dernières années, certains cas d'erreurs de gestion des certificats, des incidents de sécurité et des brèches de données les ont mis sur la sellette et ont fragilisé la puissance de ces géants. La confiance dans les certificats SSL a également été ébranlée, notamment par le fait que des organismes d'état pourraient infiltrer, dans certains cas, nos communications Web prétendument sûres.
Traditionnellement, le rôle d'une autorité de certification est de confirmer l'identité du propriétaire légitime d'un site Web avant d'émettre un certificat SSL signé. Cela reste une bonne idée pour les entreprises qui peuvent se le permettre, et certaines protections et indemnités d'assurance sont également prévues. En revanche, pour un blogueur ou un propriétaire de site professionnel lambda, il est à la fois laborieux et inutile de payer une autorité de certification et se soumettre à ce qui peut sembler un processus laborieux de vérification et de confirmation. Dans ce contexte, les alternatives techniques telles que Let's Encrypt (actuellement en phase bêta) devraient prospérer.
En outre, l'identification des faux certificats SSL va se poursuivre dans le cadre du programme de transparence des certificats de Google, grâce à des systèmes de détection intégrés dans les navigateurs Web modernes. Google continue à demander aux autorités de certification d'assumer leurs responsabilités, afin que nous soyons tous mieux protégés.
Enfin, avec l'annonce d'autres solutions telles que le protocole DANE proposé par Internet Society, qui offre la possibilité à n'importe quel propriétaire de site Web de valider son propre certificat SSL et donc de se passer totalement d'une autorité de certification, l'année 2016 va nous réserver des nouveautés intéressantes !

**Malvertising et réseaux publicitaires : réagir ou disparaître**
La publicité malveillante ou « malvertising » désigne ce qui se produit lorsque des visiteurs innocents sont la cible d'éléments malveillants, causés par des échanges avec des tiers douteux et une sécurité déficiente sur plusieurs réseaux publicitaires en ligne. En 2016, les réseaux publicitaires vont devoir réagir ou disparaître, avant qu'ils ne détruisent l'économie numérique qu'ils ont contribué à bâtir, et ne ruinent les résultats des sites Web dont la survie dépend des recettes publicitaires.
Ce problème a une cause principale : la « surface d'attaque » des scripts de publicité et de suivi toujours plus nombreux et complexes fournis par les réseaux publicitaires et intégrés par les éditeurs (souvent de façon transparente) sur leurs sites Web.
Sur mobile, plus de la moitié de la bande passante est utilisée pour la diffusion d'annonces publicitaires, beaucoup plus que pour le contenu même de la page !
S'il est associé avec des attaques réseau plus classiques, ce nouveau vecteur peut servir à infecter des milliers de victimes qui visitent des sites pourtant légitimes. Il faut aussi savoir que, même si beaucoup de grands réseaux publicitaires réagissent rapidement et arrêtent le flux de trafic lorsqu'un cas de malvertising se produit, quelques minutes suffisent pour toucher des centaines, voire des milliers de victimes. Toute personne ayant récemment installé un système de blocage publicitaire vous certifiera que ses sites Web préférés se chargent incroyablement plus vite, ce qui paradoxalement n'arrange rien.
Il faut malheureusement reconnaître qu'une grande partie des sites Web riches en contenu, pour qui les recettes publicitaires sont essentielles, se chargent lentement. En fait, une étude menée par le New York Times a montré que, pour la version mobile de nombreux sites d'actualité, plus de la moitié de la bande passante utilisée sert à la diffusion d'annonces publicitaires. Cela représente un volume de données (chargement des annonces, scripts et codes de suivi) supérieur au contenu effectivement affiché sur la page que vous lisez !
Toutefois, les systèmes de blocage de la publicité ne sont pas une solution à long terme à ce qui, finalement, est un problème de mise en œuvre. C'est encore plus vrai si vous convenez que la disparition du principe de monétisation actuellement en vigueur sur Internet pourrait avoir des conséquences économiques désastreuses. De plus, une récente déclaration de l'IAB (Interactive Advertising Bureau) confirme que les annonceurs « tiennent beaucoup moins compte de l'expérience utilisateur » dans leur manière d'élaborer des contenus.
Pour empêcher les systèmes de blocage d'annonces de se répandre, l'IAB a imaginé L.E.A.N. (de l'anglais Light, Encrypted, Ad Choice Supported and Non-Invasive), un programme basé sur des principes intervenant dans la prochaine phase des normes techniques publicitaires destinées à la chaîne d'approvisionnement publicitaire numérique globale. Quelle que soit la solution choisie, une chose est certaine : les réseaux publicitaires doivent réagir et régler les problèmes de sécurité, faute de quoi l'année 2016 pourrait bien être celle où la « vague scélérate » du malvertising aura emporté des millions d'entre nous.

**Les mots de passe résistent**
Les mots de passe sont un concept, pas une technologie, et la grande majorité d'entre nous va continuer à se servir de cet outil pour de nombreuses ressources, dans la vie privée comme dans la vie professionnelle. Alors certes, les mots de passe seront toujours utilisés en 2016, mais ils ne sont pas la panacée universelle, et vous avez donc intérêt à connaître certaines alternatives.
Cette année, Yahoo a annoncé le lancement d'une solution de sécurité qui utilise des périphériques mobiles plutôt qu'un mot de passe pour contrôler les accès, et nous avons même vu Google intégrer des fonctionnalités de verrouillage intelligent Smart Lock capables de déverrouiller votre smartphone en se servant des appareils présents à proximité.
Il existe des alternatives intéressantes aux mots de passe, même si ces derniers ont encore de beaux jours devant eux grâce à leur gratuité.
En matière de contrôle d'accès, la validation en deux étapes est un système efficace qui a tendance à se répandre et reste très utilisé chez de nombreux fournisseurs basés dans le cloud. Lorsqu'elle est proposée, vous avez tout intérêt à l'utiliser, surtout si vous n'êtes pas un spécialiste des mots de passe. Même s'il est interminable, le code de votre smartphone n'est pas inviolable, et le dispositif de lecture d'empreintes n'est peut-être pas si inutile.
Les mots de passe sont gratuits, et toutes les autres solutions ont généralement un coût, que ce soit sur le plan de la technologie ou de la complexité, ce qui explique que les mots de passe aient de beaux jours devant eux. Il est certain qu'en 2016, les problèmes liés aux mots de passe (réutilisation, stockage mal sécurisé, par exemple) ne risquent pas de disparaître. Espérons toutefois que nous saurons maintenir la vigilance des consommateurs et des entreprises !
L'Internet des objets : le principe de sécurité intégrée atteint le point d'ébullition Cela peut certes être amusant de posséder une de ces toutes nouvelles bouilloires WiFi, que vous pouvez allumer depuis votre smartphone, sans vous lever de votre fauteuil, mais ces objets normalement inoffensifs peuvent aussi révéler votre clé WiFi. Ceci n'est qu'un exemple de plus du problème existant au niveau de l'intégration de la sécurité.
S'ils ne sont pas protégés, chaque appareil périphérique, chaque téléviseur ou système stéréo intelligent, chaque système d'éclairage ou de sécurité domotique, et même ces nouveaux réfrigérateurs à la mode et ces voitures autonomes, bref tout ce qui est connecté à un réseau peut être la cible d'un hacker.
Les cybercriminels testent le matériel, analysent les ondes et recueillent mots de passe et autres données personnelles, quel que soit l'emplacement où ces informations sont conservées. Dans ce nouveau monde d'objets connectés, le danger augmente à mesure que la technologie vieillit.
Nous sommes nombreux à avoir paramétré nos ordinateurs et nos appareils mobiles de manière à ce qu'ils se mettent à jour automatiquement. En même temps, aucun d'entre nous ne pense à gérer la sécurité de ses appareils domestiques et à installer la dernière version logicielle.
Les objets connectés du quotidien peuvent réveler votre clé Wifi, et être la cible d'un hacker…Nous devons revoir notre façon de considérer ces appareils.
Dans certains cas, il est impossible de les mettre à jour. Nous devons considérer ces appareils et ces gadgets comme des ordinateurs déguisés, et les protéger aussi bien que nous le ferions pour notre PC et notre téléphone. Nous allons continuer à voir de nombreuses choses surprenantes connectées à Internet, et si aucun effort n'est fait pour y intégrer la sécurité, le problème risque d'empirer, car certains fabricants ne prennent pas le temps de mesurer les risques que courent les objets connectés au réseau.
Pour revenir un instant à l'analogie avec la bouilloire, rappelons que, dans une entreprise, si un employé achète une bouilloire intelligente, personne ne va s'en inquiéter et personne ne s'attendra à ce que le département informatique ait son mot à dire sur ce genre d'achat. Nous devons donc revoir entièrement notre façon de considérer ces appareils.

**Mettre à jour : un élément vital !**
Aujourd'hui plus que jamais, il est absolument essentiel que chaque logiciel, appareil, gadget ou équipement soit mis à jour.
Les constructeurs de voitures autonomes tels que Google annoncent déjà qu'ils assumeront la responsabilité des infractions au code de la route, et éventuellement des accidents ou des blessures corporelles dont leurs véhicules seraient responsables. Maigre consolation, avouons-le, si vous êtes victime d'un accident parce que vous avez oublié d'installer la dernière version du logiciel sur votre voiture … À mesure que les systèmes logiciels intelligents s'installent dans nos vies de multiples manières, ces mêmes logiciels pourraient décider de mettre votre vie en danger, il faut en être conscient.
Il va réellement devenir impératif que vous mettiez systématiquement vos logiciels à jour, en même temps que vos autres appareils. Un jour, cela vous sauvera peut-être la vie…

---

Réagissez à cet article

Source : *Cyber-Sécurité : AVG dévoile ses prévisions pour 2016 – Global Security Mag Online*