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*

Une célèbre PME de Montmorillon victime de piratage et de chantage

Une célèbre PME de Montmorillon victime de piratage et de chantage

Des pirates informatiques ont volé les données de clients sur le site de l'entreprise montmorillonnaise et tenté de faire chanter ses dirigeants.

Ils ne venaient pas pour les macarons et le chocolat : en début de semaine, des pirates informatiques ont attaqué le site internet de Rannou-Métivier, célèbre PME de Montmorillon. Ils visaient particulièrement la base de données de la clientèle.
« Notre service informatique a immédiatement réagi pour renforcer la sécurité du site. Cependant, des données ont déjà été volées », a fait savoir l'entreprise, mardi après-midi, dans un courrier adressé à tous ses clients disposant d'un compte sur son site.
« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »
Les intrus ont en effet enregistré des adresses de messagerie électronique et postales, ainsi que des mots de passe d'une partie des clients. Une tentative de chantage a suivi : *« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »* nous a précisé l'entreprise hier.

Les dirigeants ont en fait déposé plainte et révélé l'affaire eux-mêmes, informant les clients concernés afin qu'ils prennent leurs précautions.
« Nous vous conseillons de changer le mot de passe de votre messagerie personnelle s'il est identique à celui utilisé pour votre compte Rannou-Métivier, explique l'entreprise*. Si d'autres de vos comptes (Facebook, Ebay, Dropbox…) utilisent à la fois cette même adresse de messagerie et ce même mot de passe, nous vous conseillons d'en changer le mot de passe dans les plus brefs délais. Nous vous présentons toutes nos excuses pour la gêne occasionnée. »*

Pas de données bancaires piratées
Rannou-Métivier assure qu'aucune donnée bancaire n'est tombée entre les mauvaises mains : *« Elles n'ont jamais été stockées sur nos serveurs, elles sont utilisées uniquement le temps du paiement sur le site de la banque. Il n'y a aucun risque de perte d'argent pour nos clients. ».* La faille du site exploitée par le pirate a été identifiée mardi et la sécurité renforcée, tandis que le cryptage des données est en cours.

Rannou-Métivier emploie une soixantaine de personnes, la moitié dans ses laboratoires de production récemment agrandis à Montmorillon, le reste de l'effectif se partageant entre les boutiques de Montmorillon, Poitiers, Châtellerault et Tours.

Réagissez à cet article

Source : *Rannou-Métivier victime de piratage et de chantage – 31/12/2015 – La Nouvelle République Vienne*

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

Big Data Paris 2016

Big Data Paris 2016

Le congrès Big Data Paris 2016 se tiendra à Paris (Palais des Congrès de la Porte Maillot) le 7 et 8 mars 2016. Organisé par Corp Agency.
Le Congrès Big Data Paris vous invite, pour cette 5e année, à plonger dans l'univers passionnant du prédictif ! Sommet du Big Data en France, le congrès a réuni plus de 6 500 participants en 2015, animés par un seul et unique but : participer à la construction et au développement d'une filière française d'excellence !
Véritable laboratoire d'innovation et de disruption, le Congrès Big Data Paris 2016 valorisera les acteurs les plus avant-gardistes de la scène internationale : retours d'expériences, conférences stratégiques et prospectives, parcours immersif …
Plus d'informations sur le site de l'événement : http://www.bigdataparis.com

---

Réagissez à cet article

Source : *BIG DATA PARIS*

The Current State of Ransomware

	The Current State of Ransomware

---

In the past year or two, one of our most popular technical topics, for all the wrong reasons, has been ransomware.
Ransomware, as we're sure you know, is the punch-in-the-face malware that scrambles your files, sends the only copy of the decryption key to the crooks, and then offers to sell the key back to you.
Even Linux has ransomware these days, although fortunately we've only seen one serious attempt at Linux-based extortion so far, presuambly because cybercriminals haven't yet figured out how to make money in that part of the IT ecosystem.
Let's hope it stays that way for Linux sysadmins, because the crooks are still attacking Windows users heavily, and are still raking in lots of ill-gotten gains.

THE CRYPTOLOCKER YEARS
Two years ago, one strain of ransomware known as CryptoLocker dominated the demanding-money-with-menaces malware scene.
The US Department of Justice (DoJ) suggested that the crew behind CryptoLocker raked in $27,000,000 in September and October 2013 alone, in the first two months that the malware was widely reported.
And a 2014 survey by the University of Kent in England estimated that 1 in 30 British computer users had been hit by CryptoLocker, and that 40% of those coughed up, paying hundreds of dollars each in blackmail money to recover their data.
But in mid-2014, the DoJ co-ordinated a multi-country takedown of a notorious botnet called Gameover Zeus that targeted victims while they were doing online banking.
And, would you believe it: while the cops were raiding the Gameover servers, they came across the CryptoLocker infrastructure as well, and took down those servers at the same time, pulling off a neat double play.
CryptoLocker doesn't start its data scrambling until after it has called home for an encryption key, so killing its servers pretty much neutralised the warhead of the malware: it would get right to the very brink of detonation and then freeze, waiting for data that never came.
But any celebration about the damage done to the ransomware scene as a whole was short-lived.

RANSOMWARE REDUX
Cybercrime, if you will tolerate a clumsy metaphor, abhors a vacuum, and new ransomware soon appeared to fill the multi-million-dollar void left by the demise of CryptoLocker.
CryptoWall, and its close derivative CryptoDefense, were early pretenders to CryptoLocker's throne, but many others have appeared, too.
Threats like TorrentLocker, CTB-Locker and TeslaCrypt are big names these days, joined by other intriguing threats such as VirLock, ThreatFinder (an ironic name, considering that it is itself the threat) and CrypVault.

WHAT TO DO?
When it comes to malware of this sort, the dictum "know your enemy" is worth remembering.
With this in mind, James Wyke and Anand Ajjan, who are Senior Threat Researchers in SophosLabs, have recently published a thorough and well-written paper entitled The Current State of Ransomware.
This paper is a highly-recommended read – and it's a free download, no registration required.
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en

You'll learn about the history of ransomware, the latest threats, how they work, and what you can do to defend yourself.
Great stuff from SophosLabs!

Réagissez à cet article

Source : *The Current State of Ransomware – a new paper from SophosLabs |*

Filtrage des spams par les FAI. Possible ?

Filtrage des spams par les FAI. Possible ?

Par une ordonnance de référé concernant un litige entre Buzzee et Free, le Tribunal de commerce de Paris interdit aux FAI de bloquer les spammeurs.

Par une ordonnance de référé concernant un litige entre Buzzee et Free, le Tribunal de commerce de Paris interdit aux FAI de bloquer les spammeurs.
Voilà une jurisprudence qui peut à la fois effrayer et rassurer. Dans un litige opposant la firme Buzzee et Free en tant que Fournisseur d'Accès à Internet (FAI) et fournisseur d'un service de messagerie, le Tribunal de commerce de Paris a statué en référé pour interdire tout filtrage a priori par adresse IP des messages du premier par le second.
Certes, c'est une ordonnance de référé (statuant en urgence sur une évidence), qui plus est dans une justice spécialisée et de premier niveau. Nous sommes donc loin d'une décision de Cassation en chambre plénière. Mais les principes retenus dans cette jurisprudence portent loin puisqu'ils interdisent de fait à un FAI de filtrer les spams.

Bienvenue aux spammeurs au nom de la liberté d'expression

Buzzee est spécialisée dans l'envoi massif d'e-mails. Pour Free, c'est donc un spammeur et il a bloqué à l'entrée de ses serveurs mails tous les courriels provenant de cette entreprise en les filtrant par blocage d'adresses IP des serveurs SMTP de Buzzee. Cette dernière a donc attaqué en justice Free pour obtenir un déblocage. Et le tribunal lui a donné raison sur l'essentiel, limitant simplement ses prétentions financières exorbitantes et non-justifiées.
En effet, pour le tribunal suivant en cela l'argumentaire de Buzzee, ce n'est pas au FAI de décider qui respecte ou non la réglementation en matière de prospection commerciale, même si ses utilisateurs sont en majorité des particuliers qui doivent consentir préalablement à recevoir un message publicitaire.
Le code des postes et communications électroniques impose même une stricte neutralité aux FAI. Juridiquement, que Buzzee soit ou non un spammeur n'est pas le sujet et il n'a d'ailleurs pas été débattu. Par cette argumentation, c'est bien tout filtrage total a priori du spam qui est condamné. Au minimum, le destinataire des messages devrait donner mandat explicite à son opérateur pour filtrer selon des critères précis (comme à un opérateur de type MailInBlack par exemple). D'un autre côté, le rappel des règles de libre circulation du courrier électronique ne peut pas faire de mal. Car si un opérateur filtre le spam de sa propre initiative, on pourrait demain filtrer d'autres types de messages avec la même discrétion.

Réagissez à cet article

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*

Apprentissage :

l’intelligence artificielle, une élève de plus en plus douée

	**Apprentissage : l’ #intelligence artificielle, une élève de plus en plus douée**

Un programme informatique est-il capable, à #la manière d'un enfant, d'apprendre de son environnement ? S'il reste encore du chemin à parcourir, le machine learning, ou « apprentissage automatique », a connu des avancées significatives ces dernières années, poussé notamment par de grandes entreprises aux moyens inédits. Avec comme icône médiatique le Google Brain, qui a réussi la prouesse, en 2012, de découvrir le concept de chat en analysant des millions d'images issues du Web.

NOURRIR LE PROGRAMME : UN TRAVAIL FASTIDIEUX

La technique la plus courante de machine learning est l'apprentissage supervisé : pour qu'un programme apprenne à reconnaître une voiture, par exemple, on le nourrit de dizaines de milliers d'images de voitures, étiquetées comme telles. Un entraînement qui nécessite des heures, voire des jours, avant que le programme puisse en repérer sur de nouvelles images.

Cette technique est relativement ancienne, mais elle a fait un bond avec les récentes avancées technologiques. La masse de données désormais disponibles ainsi que la puissance de calcul à disposition des ingénieurs multiplient l'efficacité des algorithmes.

Cette nouvelle génération d'apprentissage supervisé fait déjà partie de notre quotidien : les outils de traduction automatique en sont le parfait exemple. En analysant des immenses bases de données associant des textes et leur traduction, le programme relève des régularités statistiques, sur lesquelles il se fonde pour trouver la traduction la plus probable non seulement d'un mot, mais aussi d'une formule, voire d'une phrase.

Efficace, cette méthode atteint vite ses limites. « Ces machines sont bêtes, souligne Pierre-Yves Oudeyer, directeur de recherche en robotique et sciences cognitives à l'Institut national de recherche en informatique et en automatique. Elles ne comprennent rien aux phrases qu'elles traduisent, elles ont juste vu que telle phrase était souvent traduite de telle manière. » Qui plus est, elles nécessitent un travail fastidieux de la part des ingénieurs, chargés de concevoir les gigantesques bases de données pour nourrir leur apprentissage.

QUAND UNE IA INVENTE LE CONCEPT DE CHAT

Les chercheurs en intelligence artificielle s'emploient à dépasser ces limites, pour se rapprocher de l'apprentissage humain, comme l'explique Andrew Ng :

« Si vous réfléchissez à la façon dont les enfants apprennent à reconnaître les voitures, il n'existe aucun parent, aussi attentionné et patient soit-il, qui pointera du doigt 50 000 voitures. La plupart des neuroscientifiques pensent que pour apprendre les animaux et les enfants vont dans le monde et l'expérimentent par eux-mêmes. »

C'est sur cette idée que repose le projet de deep learning Google Brain, un réseau de neurones artificiels créé en connectant pas moins de 16 000 processeurs. En 2012, soit un an après son lancement, c'est ce programme qui avait réussi à découvrir le concept de chat. Concrètement, la machine a analysé, pendant trois jours, dix millions de captures d'écran de YouTube, choisies aléatoirement et non étiquetées. A l'issue de cet entraînement, le programme avait appris à détecter des têtes de chats et des corps humains – des formes récurrentes dans les images analysées.

Lire nos explications : Comment le « deep learning » révolutionne l'intelligence artificielle

LE CAS COMPLEXE DES ROBOTS

Apprendre en expérimentant le monde : c'est la problématique à laquelle sont confrontés les chercheurs en robotique développementale et cognitive. « On tente de voir comment les robots peuvent apprendre le sens d'un mot, à travers l'expérience sensorielle et motrice, explique Pierre-Yves Oudeyer. Une chaise, par exemple, il va falloir qu'il l'expérimente, qu'il se rende compte qu'il peut s'y asseoir. »

Comme tout programme d'apprentissage, cela passe par la recherche de régularités :

« Cela peut être par exemple : "Quand je bouge mon bras de telle manière, il se passe ça." Ils pourront alors prédire les conséquences d'actions qui ne seront pas exactement les mêmes que celles déjà effectuées, dans un contexte qu'ils n'ont pas encore rencontré. »

Un sacré défi, car, contrairement au Google Brain, le robot doit collecter lui-même les expériences d'apprentissage. Impossible alors de s'entraîner sur des millions de possibilités, car cela prendrait trop de temps. Qui plus est, un robot doit être réactif à son environnement, et ne peut donc pas prendre plusieurs heures pour digérer les connaissances acquises lors de son expérience afin de préparer une réponse, qui sera entre-temps devenue obsolète.

Des expériences consistent par exemple à faire en sorte qu'un robot apprenne par lui-même à se déplacer. La machine doit expérimenter des mouvements puis enregistrer les conséquences sur son centre de gravité et son emplacement dans l'espace, puis en tirer des conclusions. Et recommencer, jusqu'à trouver la technique de déplacement la plus efficace.

Ces expérimentations peuvent être totalement aléatoires. Mais les scientifiques ont développé des algorithmes d'apprentissage actifs, « l'équivalent de la curiosité », précise Pierre-Yves Oudeyer, grâce auxquels les robots mesurent les expérimentations les plus intéressantes à effectuer pour progresser plus rapidement dans leur apprentissage. « On peut être surpris par le type de solution que le robot va trouver pour avancer. C'est parfois une solution qu'on n'avait pas imaginée, mais qui pourtant est efficace. »

« ON EST LOIN DE LA FLEXIBILITÉ D'UN ENFANT DE 5 OU 6 MOIS »

Malgré les résultats parfois impressionnants du machine learning, « le spectre de ce qu'une intelligence artificielle peut apprendre est très limité, nuance le chercheur. Le mécanisme de l'apprentissage chez l'enfant fait partie des grands mystères scientifiques, on balbutie donc dans la construction de machines dotées de capacités d'apprentissage similaires. » Pour les robots, « on est loin de la flexibilité d'un enfant de 5 ou 6 mois », prévient-il.

Et surtout, comment faire en sorte qu'un programme puisse apprendre sans l'intervention d'un ingénieur pour chaque tâche ? C'est une des grandes difficultés rencontrées dans l'apprentissage automatique :

« Aujourd'hui, on travaille sur des familles de tâches : faire qu'un robot apprenne à marcher, qu'il apprenne à attraper tel type d'objet, qu'il construise une carte d'un environnement… On développe un système ad hoc à chaque fois. Mais on ne sait pas comment une machine peut construire des représentations nouvelles pour des tâches nouvelles, comme apprendre à courir quand on sait marcher… On n'en a aucune idée. »

EN BREF :

Ce dont l'intelligence artificielle est aujourd'hui capable :

- faire évoluer ses connaissances en analysant des données ;
- découvrir des concepts en repérant seule des régularités statistiques.

Ce qu'elle ne sait pas faire :

- comprendre les concepts appris ;
- apprendre comme un enfant.

Les progrès qu'il reste à faire :

- apprendre de nouvelles tâches par elle-même ;
- développer sa curiosité.

Réagissez à cet article

Source : *Apprentissage : l'intelligence artificielle, une élève de plus en plus douée*

Quelles sont les modalités de blocage des sites Internet ?

	Quelles sont les modalités de #blocage des sites Internet ?

M. Lionel Tardy interroge M. le ministre de l'intérieur sur le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographiques.
Ce décret précise les modalités d'applications de l'article 6-1 de la loi pour la confiance dans l'économie numérique (LCEN). En complément, il souhaite savoir si, une fois la procédure appliquée, l'OCLCTIC sera également destinataire de données statistiques relatives aux tentatives de connexions aux sites bloqués, et le cas échéant, les modalités de ce recueil.

Texte de la réponse
La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a doté la France de nouveaux moyens face à la menace constante et croissante à laquelle elle est confrontée. Elle permet, notamment, de mieux combattre la propagande terroriste sur internet. Ses textes réglementaires d'application ont été rapidement publiés et toutes ses dispositions sont donc aujourd'hui applicables. Il en est ainsi des dispositions visant, suivant un dispositif gradué et équilibré garantissant le respect des libertés publiques, à renforcer les capacités de blocage des sites internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application a été publié dès le 5 février 2015 (décret no 2015-125 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique). S'agissant du nombre de connexions à un site dont l'accès est bloqué, il fait l'objet d'une comptabilisation assurée par la sous-direction de lutte contre la cybercriminalité de la direction centrale de la police judiciaire. Cette comptabilisation s'inscrit dans une démarche d'évaluation du dispositif mais vise aussi à mieux appréhender l'évolution du comportement des internautes. Lorsqu'un internaute tente de se connecter à un site dont l'accès est bloqué, il est immédiatement renvoyé sur une page d'information du ministère de l'intérieur, lui expliquant la nature du blocage et l'informant sur les voies de recours. L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste. Différents éléments peuvent expliquer cet écart. Dans la liste des sites dont l'accès est bloqué, ceux concernant la pédo-pornographie sont plus nombreux que ceux provoquant à des actes terroristes ou en faisant l'apologie (rapport de 3 pour 1). Par ailleurs, les connexions aux sites pédo-pornographiques ne sont pas toujours volontaires (liens publicitaires sur sites pornographiques légaux, « pourriels », etc.). Au-delà de ces dispositions nationales, le ministère de l'intérieur a engagé plusieurs actions à l'échelle européenne et internationale. En témoignent, notamment, les récentes rencontres du ministre de l'intérieur avec les grands acteurs américains de l'internet pour les amener à davantage participer à la régulation des contenus appelant à la commission d'actes terroristes ou en faisant l'apologie. Ces travaux ont notamment permis de décider la création d'une plate-forme de bonnes pratiques dans la lutte contre la propagande terroriste sur internet.

Réagissez à cet article

Source : *Question n°74166 – Assemblée nationale*

Le jour de la Cybersécurité maritime

Le jour de la Cybersécurité maritime

Alors qu'était publié le 25 décembre 2011 mon premier article consacré à (l'absence de) la cybersécurité dans le secteur maritime, jamais je n'aurais imaginé y revenir avec une telle régularité chaque 25 décembre depuis [1].

De là à imaginer que ce jour pourrait devenir LE jour de l'année où l'on y penserait, il n'y a qu'un pas que j'ai eu envie de franchir ! J'appelle donc solennellement de mes vœux, et en toute simplicité, qu'une autorité nationale, européenne voire internationale décrète que chaque 25 décembre soit la journée de la cybersécurité du secteur maritime.
Si mon souhait se perd dans l'immensité intersidérale du cyberespace, vous pouvez compter sur moi pour cette amicale « piqûre de rappel » aussi longtemps qu'elle sera nécessaire. En souhaitant simplement que je cesse ce rappel avant 2020 sinon cela signifiera que le niveau d'inquiétude et, surtout, de risque aura grimpé en flèche. Mais puisque c'est actuellement la trêve des confiseurs et parce que l'année 2015 aura été particulièrement difficile en France [2], essayons de rêver quelques instants.
Saluons tout d'abord la tenue des « premières rencontres parlementaires cybersécurité et milieu maritime » le 12 février 2015 à Paris, brillamment organisées par le « Cybercercle » qu'il convient ici de saluer pour son rôle et son activisme passionné. A la suite de cette journée, une lettre autour de ces rencontres, que je recommande, a été publiée [3].
Fin octobre, le colloque Safer Seas [4] a réuni à Brest l'ensemble des acteurs du secteur. Une part modeste mais somme toute bien visible [5] a été laissée à la cybersécurité notamment sous l'angle de la cybercriminalité [6].
Si, sans doute, trop nombreux sont encore les décideurs du secteur maritime à découvrir que des ports aux navires en passant par la supply chain tout ce qui embarque de l'informatique doit être soumis à interrogation, ne boudons cependant pas notre plaisir. Oui la prise de conscience a lieu et, oui, enfin, tout le monde est en train de (ou va prochainement) se mettre autour de la table pour en discuter.
La prochaine étape va donc consister à passer de la prise de conscience aux paroles, que l'on espère fortes, puis à leur concrétisation : évaluation globale des risques informatiques, audits [7], développement et insertion de services et de produits qualifiés [8], processus d'homologation [9], éducation via de la sensibilisation à l'ensemble des salariés de la filière, bonnes pratiques, etc. L'ampleur de la tâche étant si vaste [10], il faut simplement souhaiter et agir rapidement pour que les prochaines étapes ne s'effectuent pas au rythme d'une annexe à rame mais bien plus sur celui d'un hydroglisseur commandé par un capitaine expérimenté et volontaire, entouré d'un équipage adroit et tenace y compris – et surtout – au cœur des tempêtes qui s'annoncent.

[1] ou presque : 2013 puis 2014
[2] tant par les attentats de janvier et de novembre que par l'inexorable montée du chômage et la paupérisation continue d'une part croissante de nos concitoyens
[3] http://fr.calameo.com/read/004370735c23949b43ff3
[4] http://www.saferseas-brest.org/
[5] http://presse.rivacom.fr/fr/newsletter/1494/la-cybersecurite-un-enjeu-majeur-pour-le-monde-maritime
[6] http://www.letelegramme.fr/bretagne/mer/cybercriminalite-bateaux-et-ports-pour-cibles-28-10-2015-10829564.php
[7] http://si-vis.blogspot.fr/2015/02/tester-son-niveau-de-cybersecurite.html
[8] http://www.ssi.gouv.fr/entreprise/qualifications/
[9] http://www.ssi.gouv.fr/actualite/pour-homologuer-votre-systeme-dinformation-suivez-le-guide/
[1 0]
http://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/

Réagissez à cet article

Source : *Si vis pacem para bellum: Cybersécurité maritime 2015*