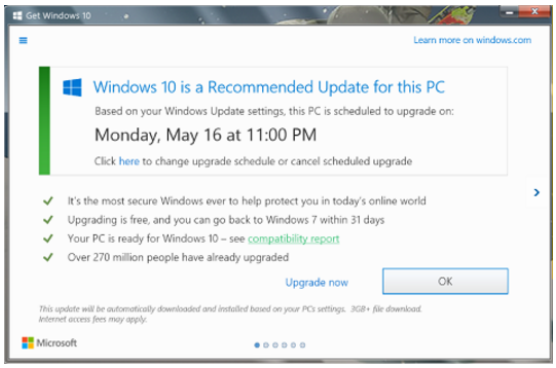
Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

	**Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?**

« Mon ordinateur m'a demandé si je voulais passer à Windows 10. J'ai cliqué sur le bouton X pour fermer la fenêtre car je ne voulais pas, et une heure après, Windows 10 est en train de s'installer. » Ce type de commentaire s'est multiplié sur les réseaux sociaux ces derniers jours. De nombreux internautes se sont plaints de voir leurs ordinateurs installer automatiquement la mise à jour vers Windows 10, alors qu'ils pensaient l'avoir refusée. Tous avaient cliqué sur la croix rouge permettant de fermer la fenêtre proposant ce téléchargement.

En général, ce bouton sert à fermer une pop-up sans avoir à donner de réponse à sa proposition. Mais depuis quelques jours, le fait de cliquer dessus a l'effet inverse : cela installe Windows 10. Une « *tromperie* », selon de nombreux utilisateurs du célèbre système d'exploitation de Microsoft.



Si l'utilisateur ferme cette fenêtre, alors Windows 10 s'installera automatiquement sur son ordinateur. Microsoft

L'entreprise, de son côté, assume et explique sur son site le fonctionnement de cette fenêtre. En fait, celle-ci fait plus que proposer une mise à jour : elle indique que la mise à jour est déjà programmée et précise la date. L'utilisateur est alors invité à cliquer sur le gros bouton « OK ». Il a aussi la possibilité, inscrite en petits caractères, de modifier la date ou d'annuler la programmation de mise à jour. Mais s'il décide simplement de fermer la fenêtre, alors Microsoft part du principe que l'utilisateur accepte la mise à jour, comme s'il avait cliqué sur « OK ».

Les utilisateurs forcés. Normal ?

Cette manœuvre de Microsoft est considérée par beaucoup comme une manière de leur forcer la main, alors que l'entreprise a annoncé sa volonté d'équiper un milliard de machines de Windows 10 en trois ans. D'autant qu'une date clé se rapproche dangereusement : à partir du 30 juillet, la mise à jour, jusqu'ici gratuite pour les utilisateurs de Windows 7 et 8, deviendra payante. Il sera alors bien plus compliqué de convaincre les sceptiques de s'y convertir.

Source : *L'étrange méthode de Microsoft pour imposer le téléchargement de Windows 10*

Réagissez à cet article

Google Chrome v51 corrige 42 failles de sécurité

	Google Chrome v51 corrige 42 failles de sécurité

Google vient de publier une nouvelle mouture stable de son navigateur Chrome, en version 51.

Chrome 51 est disponible au téléchargement pour Windows, OS X et Linux. Cette mouture intègre les interfaces de programmation Credential Management. Avec ces dernières, les sites Internet peuvent directement communiquer avec le gestionnaire de mots de passe mais aussi avec Google Smartlock ou les autorisations liées à un compte Facebook. Le processus de connexion s'en trouve simplifié, notamment sur smartphones.

L'équipe a en outre procédé à des optimisations du chargement des pages, notamment en ne récupérant pas les éléments non visibles à l'écran. Il en résulterait une meilleure gestion de la batterie avec un navigateur 30% moins gourmand.

Coté sécurité, les ingénieurs ont comblé 42 failles de sécurité en reversant au total 65 000 dollars aux experts ayant partagé leurs recherches. Retrouvez davantage d'informations sur cette page.

- Téléchargez Google Chrome 51 pour Windows
- Téléchargez Google Chrome 51 pour OS X
- Téléchargez Google Chrome 51 pour Linux

Article de Guillaume Belfiore

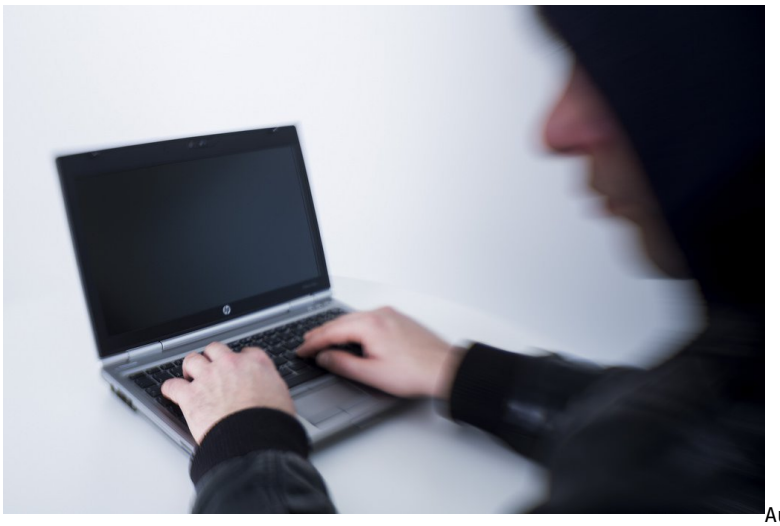
Réagissez à cet article

Source : *Chrome 51 : Google corrige 42 failles de sécurité*

La cybercriminalité fait des ravages dans les entreprises françaises.

La cybercriminalité fait des ravages dans les entreprises françaises

Selon une étude du cabinet PwC, le nombre d'entreprises françaises victimes de la cybercriminalité a presque doublé en deux ans.



Au cours des 2 dernières années, près de 70% des entreprises françaises ont été victimes de fraudes. On note notamment une forte hausse de la cybercriminalité, selon une étude effectuée par le cabinet Price Water House Coopers (PwC) publiée hier. La moyenne nationale est beaucoup plus élevée que celle mondiale.

La cybercriminalité visant les entreprises françaises explose

Les entreprises françaises sont-elles des cibles faciles pour les pirates ? Selon une étude de Price Water House Coopers concernant les fraudes en entreprises, les attaques informatiques occupent le deuxième rang derrière le détournement d'actifs. En 2 ans, la cybercriminalité a explosé en France, elle représente 53% des fraudes en 2016 contre 28% en 2014.

Aujourd'hui, une grande partie des entreprises (85%) ont pris conscience que le risque d'être victime de pirates informatiques est bel et bien réel. Elles n'étaient que 48% en 2014. Selon Louis Di Giovanni, travaillant dans le département Litiges et Investigations du cabinet PwC, « L'explosion du Big Data quels que soient les domaines, alliée à la digitalisation de l'activité économique et la multiplicité des supports numériques augmentent l'exposition des entreprises au risque de cyberattaque, d'où une plus grande prise en compte de ce risque par les dirigeants« .

Les entreprises françaises ne sont pas prêtes face à ce risque

Bien que les entreprises françaises aient bien pris en compte le risque élevé que représente la cybercriminalité, elles n'ont pas forcément mis en place de défenses adéquates. « Plus de la moitié des entreprises françaises n'ont pas encore de plan d'action 100% opérationnel pour répondre à une cyberattaque » déclarait M. Di Giovanni.

A cause de l'explosion de la cybercriminalité, le taux de fraude en entreprise progresse fortement. 68% des entreprises ont déclaré avoir été victimes d'une fraude au cours des deux dernières années, contre 55% en 2014, soit une hausse de 13 points… [Lire la suite]

L'étude PWC Global Economic Crime Survey 2016

Réagissez à cet article

Source : *La cybercriminalité fait des ravages dans les entreprises françaises*

Auteur : David Pain

Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint

Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. — Entreprises Numériques

---

Impossible d'échapper aux mécanismes de recommandations sur Internet. Tous les sites internet, marchands ou réseaux sociaux, utilisent désormais ces fameuses recommandations censées influencer nos comportements d'achats. Basées sur de l'intelligence artificielle de plus en plus puissante, les recommandations se font plus pertinentes. Dans l'avenir elles pourront tirer profit d'une connaissance précise de notre personnalité comme le montre une étude réalisée à partir de l'analyse des « likes » de Facebook.

Toute action sur Internet se transforme en données. On s'inquiète à juste titre de l'usage qui est fait de nos données personnelles (voir mon billet sur Safe Harbor). L'annonce par Facebook de « Search FYI » devrait encore attirer notre attention sur la protection de notre vie privée. Avec Search FYI, Facebook peut rechercher des informations dans tous les messages publics publiés par ses membres. Avec le développement de l'intelligence artificielle et l'utilisation du machine learning la valeur des données monte en flèche. Le mot « donnée » est souvent sous-estimé. On comprend bien qu'une photo et un texte postés sur un réseau social sont des données mais on oublie que le simple fait de cliquer sur un « like » devient une donnée aussi importante voire plus. Toute action sur internet laisse une trace numérique qui pourra être exploitée. C'est la base même du marketing digitale qui utilise ces traces numériques laissées sur le parcourt client pour mieux connaitre le consommateur et augmenter l'expérience utilisateur. C'est du donnant donnant : mieux nous sommes connus, mieux nous sommes servis. C'est l'évolution naturelle liée à la transformation numérique.
En analysant les « Likes », Facebook en sait plus sur notre personnalité que nos proches. La personnalité est un concept complexe qui semble difficilement mesurable. Cela touche à des sentiments, des émotions, des valeurs qui nous façonnent et qui nous rendent uniques. On pourrait donc imaginer, voire espérer, que les ordinateurs puissent se montrer impuissants à « quantifier » ce qui nous définit en tant qu'être humain. Pourtant une étude menée par des chercheurs des universités de Cambridge et de Stanford, publiée en janvier 2015, a montré que l'Intelligence Artificielle a le potentiel de mieux nous connaitre que nos proches. Cette étude visait à comparer la précision d'un jugement sur la personnalité réalisé par un ordinateur et des êtres humains. Les chercheurs ont demandé à 86.200 volontaires de leur donner accès à leurs « Likes » sur Facebook et de répondre à un questionnaire de 100 questions sur leur personnalité. Ces données ont été modélisées et le résultat est assez étonnant. On apprend que :
Avec l'analyse de 10 likes, Facebook en sait plus sur nous que nos collèges
Avec 70 likes Facebook en sait plus que nos amis
Avec 150 likes Facebook en sait plus que notre famille
Avec 300 likes Facebook en sait plus que notre conjoint
Quand on sait qu'en moyenne un utilisateur Facebook a 227 Likes, on se dit que nous n'avons plus grand choses à cacher.
Partager des émotions comme on partage des photos ou des vidéos. C'est la prochaine étape qu'imagine Mark Zuckerberg dans le futur. Durant une session de questions réponses sur son profile Facebook, le patron de Facebook a expliqué qu'il pensait que nous aurions à l'avenir la possibilité de partager nos expériences émotionnelles rien que par le seul fait d'y penser. La télépathie appliquée aux réseaux sociaux ? En matière d'Intelligence artificielle il devient difficile de faire la différence entre science-fiction et prévision. Quoiqu'il en soit Gartner a rappelé que c'étaient les algorithmes qui donnaient leur valeur aux données. Le progrès de ces algorithmes et leur complexité justifient qu'on s'intéresse à la protection de notre vie privée. Ils deviennent incontournables dans notre vie moderne, il faut en être conscient… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques*

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

---

Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.

Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au coeur d'une controverse d'experts.
Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités.
Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.
Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».
« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les liberté civiles.

L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.
Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thaï Duong.
Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »… [Lire la suite]

Réagissez à cet article

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël

Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël m

Noël 2016 sera encore placé sous le signe des gadgets roulants électriques. Au MedPi, les constructeurs alignent leurs gammes .

On ne découvre pas vraiment des produits que l'on ne connaissait pas au MedPi, mais comme il s'agit avant tout du supermarché des professionnels de la distribution, il est possible de sentir les tendances qui se dessineront pour les événements commerciaux français à venir – et en particulier la rentrée et Noël. Quand on découvre un gadget incroyable et qu'il n'est pas disponible en France, on sait que son adoption sera lente, réservée aux passionnés. Ici, nous sommes dans le réel, dans les rayons des grands magasins. Et le réel, en 2016, c'est beaucoup de choses qui roulent.
Si vous aviez des enfants en âge de commander un hoverboard à Noël dernier, vous pouvez être sûr qu'ils ne passeront pas à côté de la deuxième génération de ces produits qui ont envahi les rayons et se classent en premier rang des vidéos de chutes ridicules sur YouTube. En tout cas, au MedPi, on ne peut pas parcourir une allée sans voir au moins une marque ou un importateur qui cherche à placer dans les rayons ses engins à roues uniques, double roues parallèles, double roues sur un axe, double roues sur un axe avec selle… la liste est longue.

L'idée derrière ces engins ne différencie pas vraiment entre les modèles : il s'agit d'exploiter les performances actuelles des moteurs électriques et des batteries pour proposer des engins qui répondent aux problématiques de la mobilité urbaine. Il faut pouvoir se déplacer rapidement, sans risque majeur de chute… et sans effort. Ce dernier point pourrait paraître regrettable, mais nous nous sommes aperçus dans notre premier test d'une trottinette électrique qu'elle ne remplaçait pas, naturellement, les trajets que l'on aurait fait à pied ou en vélo, mais bien plus volontiers les trajets en transports en commun. En somme, les plus pénibles.
Bien entendu, sur ce secteur, le bon grain côtoie l'ivraie. Les marques les plus réputées comme Ninebot, qui possède Segway, ont des brevets et de nombreuses innovations dans leur portefeuille en plus d'avoir des appareils de grande qualité, autostabilisés. Les autres rattrapent leur retard ou proposent des ersatz de technologies pas vraiment convaincantes (ni légales), laissant sur le carreau tout le côté stable des engins qu'ils proposent, les faisant entrer dans la catégorie « jouets pour ados » plus que dans celle de la mobilité urbaine. Et pour un Ninebot ou équivalent, il y a au moins 3 constructeurs aux noms étranges dans les allées du MedPi.
Plusieurs problématiques restent d'ailleurs à résoudre pour que ce marché explose véritablement. La première, c'est bien entendu la question de la sécurité des utilisateurs : les hoverboards qui ont assailli l'Europe et les États-Unis l'an passé étaient loin d'être tous conformes aux régulations en vigueur en matière d'électronique et plusieurs affaires de batteries défectueuses ou anormalement inflammables avaient conduit au bannissement de certains modèles, notamment vendus par Amazon.
Ensuite vient la route – ou les trottoirs. Où doivent rouler ces engins ? Sur les trottoirs, ils peuvent être dangereux pour les piétons et pour eux-mêmes, dans la mesure où les voies piétonnes sont pavées d'obstacles contre lesquels les personnes en chaise roulante doivent lutter depuis longtemps, malheureusement. Sur la route, c'est l'utilisateur qui devient vulnérable, debout en équilibre, lancé à plusieurs dizaines de kilomètres par heure. On l'imagine mal à l'aise dans les croisements. Si les voies pour les vélos étaient massivement installées, comme chez nos voisins hollandais, la question ne se poserait pas.
En France, elle est encore ouverte : peut-être est-il temps que les municipalités s'en emparent avant que nous ayons à écrire des articles sur les premiers accidents graves. Même si les hoverboards ne volent (presque) toujours pas… [Lire la suite]

Réagissez à cet article

Source : *Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël – Tech – Numerama*

Vers une nouvelle plainte européenne contre Google

Vers une nouvelle plainte européenne contre Google

Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

Réagissez à cet article

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*

BMW lance un défi aux startups françaises pour améliorer la voiture de demain

	**BMW lance un défi aux startups françaises pour améliorer la voiture de demain**

Le BMW Tech_Date, prévu pour le 9 juin prochain, est un concours ouvert aux startups françaises. Ces dernières doivent y présenter des innovations intégrables dans les voitures intelligentes conçues par le constructeur.

BMW sollicite les startups françaises. Le constructeur automobile organise le 9 juin prochain la première édition du BMW Tech_Date dans son magasin des Champs Élysées à Paris. L'objectif : accélérer la construction de la mobilité des cent prochaines années.
Ce concours permettra aux startups de présenter des innovations qu'elles pensent pouvoir intégrer aux futures voitures intelligentes de BMW. C'est en tout cas ce que souhaite le constructeur.
« Nous avons les technologies pour rendre la voiture intelligente mais nous sommes en recherche constante de solutions qui peuvent rendre l'usage de la voiture plus intelligent », explique Pierre Jalady, responsable marketing de BMW en France, dans une interview au Journal du Net. L'entreprise souhaite en effet adapter ses services pour qu'ils soient plus centrés sur l'utilisateur.
Les startups ont jusqu'au 30 mai pour candidater. Une vingtaine d'entre elles seront sélectionnées pour le Tech_Date afin de présenter leurs technologies devant un jury qualifié.

Trois vainqueurs seront désignés en fonction de plusieurs critères dont :
• niveau d'innovation de la solution proposée
• le délai d'intégration potentiel pour BMW
• D'autres éléments seront pris en compte tels que le niveau préexistant de relations commerciales avec l'industrie automobile, la solidité de la société et la communauté fédérée par les startups sur les réseaux sociaux.
Les trois gagnants « seront reçus pendant une semaine au siège de Munich, où ils rencontreront toutes les équipes qui auront un intérêt à travailler avec eux, des achats au marketing. Ils seront aussi mis en avant au Mondial de l'automobile de Paris en octobre prochain », affirme Pierre Jalady.
Ce concours a également pour but de célébrer le siècle d'existence de BMW qui fêtait son anniversaire en mars dernier. Le constructeur estime que le Tech_Date est une occasion de mettre en lumière les innovations françaises et déclare vouloir travailler en partenariat avec les entreprises les plus créatives.
Crédit photo de la une : BMW… [Lire la suite]

Réagissez à cet article

Source : *BMW lance un défi aux startups françaises pour améliorer la voiture de demain – Tech – Numerama*

Les métadonnées téléphoniques très bavardes sur notre vie privée

Les métadonnées téléphoniques très bavardes sur notre vie privée

---

Les métadonnées téléphoniques révèlent des informations très privées

Une équipe de chercheurs de l'université de Stanford a publié une vaste étude montrant l'étendue des informations personnelles qui peuvent être déduites des seules métadonnées de ses appels et SMS sur la vie privée d'une personne. A savoir toutes les informations qui « entourent » un message : durée d'un appel, numéro appelé, heure de l'envoi d'un SMS… En bref, tout ce qui concerne un message, à l'exception de son contenu.
En 2013, le lanceur d'alerte Edward Snowden avait révélé que la NSA, les services secrets américains, et leurs partenaires procédaient à une surveillance de masse de ces métadonnées, enregistrant quotidiennement les informations autour de millions de messages. La NSA affirme depuis 2013 que ces informations ne revêtent pas un caractère privé, mais qu'elles sont indispensables à l'efficacité de ses actions, notamment en matière de lutte contre le terrorisme.
Les conclusions de l'étude menée par les chercheurs de Stanford montrent tout le contraire. Pendant plusieurs mois, ils ont enregistré, avec l'accord des 823 participants à l'étude, les métadonnées de 251 788 appels et de 1 234 231 SMS. Ils ont ensuite analysé de manière automatique les tendances récurrentes dans les métadonnées. Des appels réguliers à des commerces dans une zone géographique précise peuvent par exemple indiquer que la personne habite dans ce quartier. Les chercheurs ont ensuite procédé à des analyses « manuelles » pour identifier des numéros appelés et tenter d'en déduire des informations sur la vie privée des participants.

GROSSESSE, PROBLÈME CARDIAQUE, ARMES À FEU…

Ils sont ainsi parvenus à déterminer que l'un des participants venait de se voir diagnostiquer un problème cardiaque : après un long appel à un centre de cardiologie, l'homme avait appelé un laboratoire médical, puis reçu plusieurs coups de fil d'une pharmacie, avant d'appeler le service consommateur d'une entreprise qui commercialise des outils permettant de surveiller son rythme cardiaque. Dans d'autres cas, la seule analyse des métadonnées a permis de montrer l'existence de grossesses, ou le fait qu'une personne avait acheté une arme à feu.
Les analyses automatiques des données se sont révélées moins précises : la technique n'a permis d'identifier la ville où résident les participants à l'expérience que dans 57 % des cas – mais dans 90 % des cas, l'analyse a permis de déterminer la localisation des personnes à moins de 80 km de leur domicile réel.
Interrogé par le Guardian, l'un des coauteurs de l'étude, Patrick Mutchler, affirme que ces résultats sont bien en deçà de ce dont sont capables les agences de renseignement, qui disposent de moyens considérables. « Gardez à l'esprit que [ces résultats] ne sont que le reflet de ce que peuvent faire deux doctorants disposant de ressources limitées. »… [Lire la suite]

Réagissez à cet article

Source : *Les métadonnées téléphoniques révèlent des informations très privées*

Et si la reconnaissance faciale de Facebook était excessive ?

Et si la reconnaissance faciale de Facebook était excessive ?

Depuis 2010, Facebook propose à ses utilisateurs un système de reconnaissance faciale qui permet de gagner du temps dans le « taguage » des personnes qui sont sur les photos. Sous couvert d'une nouvelle fonctionnalité, c'est un véritable dispositif biométrique qui a été mis en œuvre car il permet d'identification d'un individu à partir d'une simple photographie de son visage.

En Californie, trois utilisateurs ont reproché au réseau social n°1 d'avoir « secrètement et sans leur consentement » collecté des « données biométriques dérivées de leur visage ». Ces plaintes ont été jugées recevables par le juge James Donato qui « accepte comme vraies les allégations des plaignants » et juge « plausible » leur demande.

Au sein de l'Union européenne, le danger a rapidement été perçu s'agissant du système de reconnaissance faciale de Facebook qui l'a suspendu en 2012. Mais aux Etats-Unis, bien moins vigilants, cette fonctionnalité a perduré et il apparait bienvenu que la Justice y réagisse enfin. Facebook a constitué des profils qui répertorient les caractéristiques du visage de ses utilisateurs, leur cercle d'amis, leurs goûts, leurs sorties, etc. Avec plus de 3 milliards d'internautes dans le monde, cela revient à ce qu'environ 28% de la population ait un double virtuel rien que sur Facebook.

Facebook is watching you : Reconnaissance faciale, intelligence artificielle et atteinte aux libertés

Eu égard à leur grand potentiel discriminatoire, les données biométriques sont strictement encadrées par la loi du 6 janvier 1978 puisque d'après son article 25, une autorisation préalable de la Commission nationale de l'informatique et des libertés est indispensable pour mettre en œuvre des « traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ». Cela regroupe l'ensemble des techniques informatiques qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les conditions générales d'utilisation de Facebook ne sont pas donc pas conformes à la législation française sur les données personnelles, notamment s'agissant de la condition de consentement préalable, spécifique et informé au traitement des multiples données à caractère personnel collectées. Mais le géant de l'internet ne répond qu'à l'autorégulation. Par opposition à la règlementation étatique, la régulation n'entend prendre en compte que la norme sociale, c'est-à-dire l'état des comportements à un moment donné. Si la norme sociale évolue, alors les pratiques de Facebook s'adapteront.

Vers une remise en cause mondialisée des abus de Facebook ?

L'affaire pendante devant les Tribunaux met en lumière le manque de réactivité des américains face aux agissements de Facebook. C'est seulement au bout de 5 années que la Justice s'empare de la question des données biométriques à l'initiative de simples utilisateurs, alors même qu'une action de groupe à l'américaine d'envergure aurait pu être engagée pour mettre sur le devant de la scène les abus de Facebook.

Néanmoins, « mieux vaut tard que jamais » et l'avenir d'une décision répressive ouvre la porte vers de nouveaux horizons pour l'ensemble des utilisateurs. En effet, Facebook prend comme modèle pour toutes ses conditions générales d'utilisation à travers le monde la version américaine de « licencing ». Plus Facebook se verra obligé dans son pays natal à évoluer pour respecter les libertés individuelles des personnes inscrites, plus on s'éloignera du système tentaculaire imaginé par Mark Zuckerberg qui n'est pas sans rappeler celui imaginé par Georges Orwell dans son roman 1984.

Par Antoine CHERON, avocat associé, est docteur en droit de la propriété intellectuelle, avocat au barreau de PARIS et au barreau de BRUXELLES et chargé d'enseignement en Master de droit à l'Université de Assas (Paris II). Il est le fondateur du cabinet d'avocats ACBM… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Facebook is watching you : système biométrique efficace – Data Security BreachData Security Breach*