Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester

Les débordements lors des manifestations organisées chaque semaine contre le projet de loi Travail ont fait réagir Bruno Retailleau. Le sénateur LR vient de déposer une proposition de loi pour instituer notamment un nouveau fichier, celui des interdits de manifester.

Manifester paisiblement, oui, dans la violence, non. Tel est l'angle du texte déposé la semaine dernière par le parlementaire de l'opposition. Son auteur réprouve le fait que désormais, « *les forces de l'ordre sont, de façon répétée, prises pour cible à l'occasion de ces rassemblements* ». Et selon lui, « *un palier dans l'expression de la violence a été franchi, le 18 mai dernier, au cours d'une manifestation interdite lors de laquelle deux fonctionnaires de police ont été lâchement pris à partie et violemment agressés* ».

Dirigée contre les « *casseurs* », dixit son introduction, cette PPL s'inspire du mécanisme existant à l'encontre des hooligans. Le premier article veut ainsi permettre aux préfets de prononcer une mesure d'interdiction de manifester à l'encontre de toute personne « *ayant pris une part active dans un précédent attroupement en cherchant à entraver, par la force ou la violence, l'action des pouvoirs publics* » ou « *impliquée dans la commission d'un acte de dégradation ou de violence à l'occasion de l'une de ces manifestations* ». L'arrêté s'étendrait jusqu'à 12 ou 24 mois selon le comportement de la personne.

Un fichier des interdits de manifester

Pour épauler l'interdiction, qui doit être validée par un vote de l'Assemblée nationale et du Sénat, un traitement automatisé serait nourri de ces arrêtés d'interdiction, mais aussi des noms des personnes condamnées à la peine d'interdiction de participer à des manifestations sur la voie publique (L. 211-13 Code de la sécurité intérieure).

Après passage par la CNIL, sa finalité serait « *de prévenir les troubles à l'ordre public, les atteintes à la sécurité des personnes et des biens ainsi que les infractions susceptibles d'être commises à l'occasion des manifestations sur la voie publique et des rassemblements en lien avec ces manifestations se tenant dans le ressort de leur département* ».

Accentuation du périmètre de la « vidéoprotection »

Ce n'est pas tout. L'article 3 vient modifier le régime de la « vidéoprotection ». À ce jour, le Code de la sécurité intérieure autorise « la transmission et l'enregistrement d'images prises sur la voie publique » lorsqu'il s'agit d'assurer « la protection des bâtiments et installations publics et de leurs abords », « la sauvegarde des installations utiles à la défense nationale », « la constatation des infractions aux règles de la circulation », la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés, ou encore la prévention d'actes de terrorisme.

La proposition de loi aimerait ajouter au long inventaire, « *la prévention des troubles à l'ordre public en cas de manifestation sur la voie publique, au besoin au moyen de dispositifs mobiles* ». Pourquoi ? Selon le parlementaire, « *visionner la voie publique ou un lieu ouvert au public n'est possible que dans des cas et pour des motifs définis par la loi. [Cet article] rend possible la mise en œuvre d'un système de vidéo-protection sur le parcours et aux abords immédiats d'une manifestation. Afin d'assurer la faisabilité technique du dispositif, il est prévu de recourir à des caméras mobiles. L'arrêté d'autorisation déterminera la position de chacune des caméras et la période de temps au cours de laquelle le dispositif pourra être utilisé.* »

« Des objets susceptibles de constituer une arme »

La PPL s'intéresse tout autant au Code pénal, et spécialement à l'article concernant la participation délictueuse à une manifestation. Aujourd'hui, il punit de trois ans de prison de prison et 45 000 euros d'amende le fait d'y prendre part en étant porteur d'une arme.

Pour mieux assurer la préservation de l'ordre public, Bruno Retailleau y ajoute le fait « *d'introduire, de détenir ou de faire usage de fusées ou artifices de toute nature ou d'introduire sans motif légitime tous objets susceptibles de constituer une arme* » et celui « *de jeter un projectile présentant un danger pour la sécurité des personnes dans une manifestation sur la voie publique*», sachant que « la tentative de ces délits [sera] punie des mêmes peines ».

Toujours dans cette optique, elle rêve également d'instaurer une prune de 3 750 euros pour quiconque aura introduit ou consommé de l'alcool dans une manifestation sur la voie publique ou participé à une telle réunion « *en état d'ivresse* ».

Provocation à la haine contre les policiers

Outre un élargissement des possibilités d'interdire une personne à participer à des réunions et une obligation de pointage pour les personnes condamnées par un tribunal, la loi de 1881 sur la presse profite également d'une mise à jour. L'idée ? Ériger en infraction le fait de provoquer à la discrimination, à la haine ou à la violence à l'égard d'une personne « *à raison de sa profession* » (jusqu'à un an d'emprisonnement ou/et de 45 000 euros d'amende).

Pour le cas présent, la profession visée est évidemment celle des gendarmes et des policiers. Seront donc concernés ceux qui auront incité, notamment sur Internet, à la haine à l'égard des forces de l'ordre. Le dernier article prévoit d'ailleurs d'instaurer une période de sûreté pour les auteurs de violences contre elles.

S'assembler oui, mais « paisiblement »

Pour justifier son texte, Retailleau se souvient que « *l'article 7 de la Déclaration des droits de l'homme et du citoyen consacre 'le droit de s'assembler paisiblement'* ». Dans le texte fondateur, le principe est plutôt inscrit à l'article 10 (« *Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi* »).

Les adversaires d'un tel dispositif se rappelleront que la Déclaration de 1789 prévoit aussi que « *la Loi ne doit établir que des peines strictement et évidemment nécessaires* » (article 8) sachant que quiconque a le droit de résister à l'oppression (article 2) et que « *la garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée* » (article 12).

Merci à Marc Rees, auteur de cet article

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

- 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

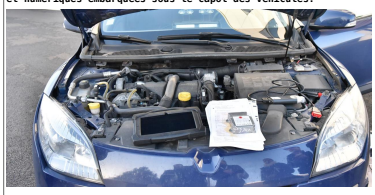
Contactez-nous

Réagissez à cet article

Source : *Pour prévenir les violences, un sénateur veut un fichier des interdits de manifester – Next INpact*

Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact

L'Ordinateur de bord de votre voiture n'aura bientôt plus de secret pour les autorités. Une disposition adoptée dans le projet de loi sur la justice du XXIe siècle va autoriser gendarmes et policiers à fouiller les données physiques et numériques embarquées sous le capot des véhicules.



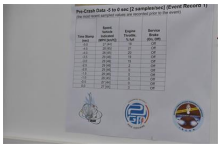
C'est un champ d'investigation suivi de près par les autorités, comme cela a pu nous être expliqué en janvier dernier, lors d'une visite au Pôle judiciaire de la Gendarmerie nationale de Cergy-Pontoise. Dans les véhicules les plus récents, les agents peuvent techniquement scruter tous les relevés techniques glanés quelques secondes avant un accident de la route. Vitesse, direction, freinage, etc. sont une mine d'informations pour confirmer ou fragiliser les affirmations du type : « *je roulais à 50 km/h, j'ai immédiatement freiné lorsque j'ai vu la future victime traverser la route* ».

Dans le projet de loi sur la justice du XXIe siècle, un amendement du gouvernement pousse davantage encore l'usage de ces investigations. Ce texte, numéroté CL180, avait été adopté en commission des lois début mai. Il a été conservé en l'état lors de la séance publique, la semaine dernière :
« *Art. L. 311-2. – Les agents compétents pour rechercher et constater les infractions au présent code, dont la liste est fixée par décret en Conseil d'État, ont accès aux informations et données physiques et numériques embarquées du véhicule afin de vérifier le respect des prescriptions fixées par le présent code* ».

L'article intègrera le titre Ier du Code de la route relatif aux dispositions techniques. Il autorisera les agents, désignés par décret, à avoir un plein accès aux données physiques et informatiques de votre véhicule. Pour cela, ils n'auront qu'à justifier de la recherche ou de la constatation d'une infraction au Code de la route. Si la pêche est bonne, alors on passera du contrôle à la possible sanction.

La cible, le diagnostic embarqué… mais pas seulement

Dans son exposé des motifs, le gouvernement souligne qu'il s'agit d'ouvrir « *notamment* » un accès « *aux systèmes de diagnostic embarqués* ». Concrètement, via un ordinateur portable connecté sur la prise de l'ordinateur de bord, policiers et gendarmes pourront prendre connaissance des données issues « *notamment* » des capteurs.



Analyses menées à Cergy-Pontoise Crédits : Marc Rees (CC BY SA 3.0)

Selon l'exécutif, la proposition a été soufflée par le comité interministériel de sécurité routière. Seulement, s'il l'envisage « *dans le cadre du contrôle du respect des dispositions techniques liées aux véhicules* », son texte est bien plus large. Le gouvernement a d'ailleurs ajouté cette phrase, à la fin de l'article : « *le fait que ces opérations révèlent des infractions autres que celles visées au premier alinéa ne constitue pas une cause de nullité des procédures incidentes* ». En clair, en recherchant des infractions au Code de la route, les agents pourront en toute quiétude découvrir d'autres éléments illicites, par exemple planqués dans un disque dur connecté au véhicule.

La latitude est d'autant plus large que n'est pas spécifié l'art et la manière dont aura lieu l'accès. Celui-ci pourra donc se faire par liaison physique (connexion par câble sur la prise du système embarquée), ou pourquoi pas à distance, avec le développement des véhicules connectés.

Le Syndicat de la magistrature réclame un encadrement de l'accès

De son côté, le Syndicat de la magistrature se dit « *hostile à l'introduction d'un [tel] article donnant accès aux informations et données physiques et numériques embarquées du véhicule sans autre condition que « pour rechercher et constater les infractions au présent code » et en permettant que les infractions révélées incidemment puissent être utilisées alors même qu'elles ne correspondent pas à celles recherchées* ». Selon le SM, une telle extension en effet, « *ne saurait être ainsi avalisée, sans aucun contrôle de nécessité ou de proportionnalité, ni procédure encadrant ces accès* ».

Adopté par les députés, mais non encore par les sénateurs, cet article va faire l'objet d'un arbitrage en Commission mixte paritaire dans les prochains jours.

Fichier des assurances, contrôles par lecture automatisé des plaques

Toujours dans le secteur de l'automobile, le même projet organise également la création d'un fichier des assurés, qui sera exploité par les dispositifs de contrôle automatisés et de vidéoverbalisation.

Un autre projet de loi, celui sur la réforme pénale a, lui, augmenté les hypothèses où les services de police, de gendarmerie nationale et des douanes pourront mettre en place une LAPI (ou Lecture automatique de plaques minéralogiques) ainsi qu'une prise photographique des occupants d'un véhicule. Ces hypothèses sont celles inscrites à l'article 706-73-1 du Code de procédure pénale, à savoir l'escroquerie en bande organisée, le travail dissimulé, le blanchiment, et même la non-justification des ressources… [Lire la suite]

Merci à Marc Rees, l'auteur de cet article

Réagissez à cet article

Source : *Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact*

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse a trouvé possiblement une solution radicale pour lutter contre la présence des téléphones portables dans les prisons : elle veut tout simplement pouvoir faire désactiver la carte SIM en cause dans les mains des opérateurs.

Les tribunaux de shérif d'Écosse (ou «Sheriff courts») auront bientôt la compétence de contraindre les opérateurs télécoms à déconnecter les téléphones portables non autorisés dont on détecterait une utilisation en prison. Concrètement, le tribunal ordonnera à l'opérateur de réseaux de désactiver ou déconnecter un téléphone mobile et/ou une carte SIM. C'est le sens d'un texte qui vient d'être notifié à Bruxelles, cette disposition imposant une restriction normative dans un État membre.

Accéder aux réseaux sociaux, intimider les témoins

« *Des détenus ont utilisé des téléphones portables non autorisés pour accéder aux réseaux sociaux, intimider des témoins et poursuivre et contrôler leurs activités criminelles depuis les institutions pénitentiaires,* expliquent les autorités écossaises en appui de leur texte. *Ils représentent par conséquent une menace notable pour la sécurité et le bon fonctionnement des établissements pénitentiaires.* »

Le hic est qu'actuellement, « *il est extrêmement difficile de trouver à l'intérieur d'institutions pénitentiaires des cartes SIM en raison de leur taille. Si c'est moins le cas pour les téléphones portables, ces détenus qui ont pris possession de téléphones portables seront prêts à faire l'impossible pour empêcher la détection desdits téléphones, notamment par des menaces et l'intimidation d'autres personnes.* »

En France, le projet de loi sur la réforme pénale

Le texte pourra entrer en vigueur dans trois mois, une fois achevé le round de la notification bruxelloise. En France, si les pouvoirs du juge profitent théoriquement d'une large latitude pour ordonner ce type de mesure, dans le projet de loi sur la réforme pénale, la réaction du législateur gagne plusieurs crans au-dessus par rapport aux textes antérieurs.

D'un, le pénitentiaire va devenir un service du renseignement. De deux, les autorités, qu'elles soient judiciaires ou administratives et sans qu'on sache très bien où se placera la frontière de leurs compétences, pourront installer une ribambelle de dispositifs techniques pour détecter des communications, et notamment des IMSI catchers. De là, elles seront en capacité d'effectuer des interceptions de sécurité pour prendre connaissance des correspondances échangées avec l'extérieur, etc… [Lire la suite]

Marc Rees auteur de cet article

Réagissez à cet article

Source : *L'Écosse veut désactiver les téléphones utilisés en prison – Next INpact*

La Cnil accorde un sursis à

Facebook pour faire preuve de loyauté (ou pas)

	La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas)

Alors qu'il s'apprête à lancer de la publicité ciblée hors de ses services, y compris auprès des non-utilisateurs de sa plateforme, Facebook a obtenu un sursis de 3 mois de la Cnil. L'autorité lui reproche une collecte déloyale de données personnelles.

Le réseau social a été mis en demeure le 9 février par l'autorité française de protection des données personnelles. La Cnil reproche à Facebook une collecte déloyale de données de navigation d'internautes non membres et l'absence de recueil d'un consentement pour le croisement de données à des fins publicitaires.
La firme de Mark Zuckerberg disposait d'un délai de trois mois pour se mettre en conformité. Mais d'après le JDN, Facebook a sollicité auprès de la Cnil un délai supplémentaire de trois mois. Celui-ci lui a été accordé.

Sécurité et publicité grâce au même cookie finalement

« Nous avons repoussé au 9 août le délai obligatoire pour se mettre en conformité » répond la Cnil. Sur le plan commercial, Facebook se montre plus dynamique. La société a annoncé tout récemment un changement de cap.
Elle entend en effet proposer de la publicité ciblée à tous les internautes et non uniquement à ceux inscrits sur son réseau. Pour suivre ces internautes,Facebook met à profit son cookie Datr. La firme assurait pourtant jusqu'à présent que ce cookie avait pour seule finalité la sécurité.
Plus d'ambiguïté à présent. Le réseau social précise que sa régie publicitaire, Audience Network, suivra dorénavant l'ensemble des internautes via ses cookies « même ceux qui ne disposent pas de compte Facebook ou ne s'y connectent pas. »… [Lire la suite]
Merci à ZdNet

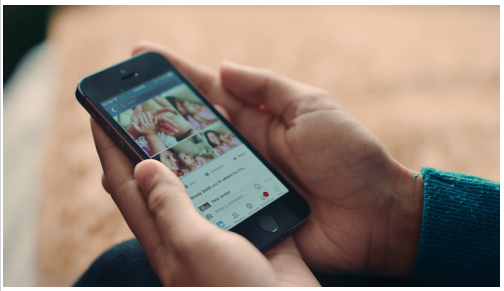
Réagissez à cet article

Source : *La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas) – ZDNet*

Facebook vous traque sur le Web même si vous n’êtes pas membre

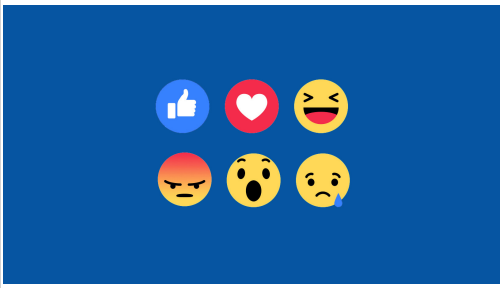
Facebook vous traque sur le Web même si vous n’êtes pas membre

Facebook devient une régie publicitaire ouverte aux sites tiers, et affichera des publicités ciblées y compris pour les internautes qui ne sont pas inscrits sur le réseau social. Il utilisera ses scripts présents sur de nombreux sites pour suivre l'internaute dans ses déplacements sur le Web, et comprendre ce qui l'intéresse.

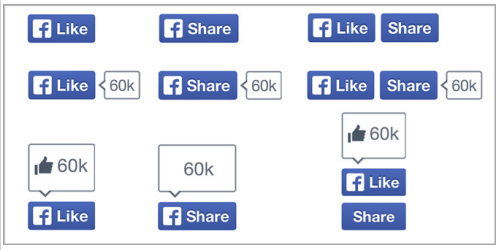


On connaît tous une ou deux personnes qui se refusent à utiliser Facebook et échappent encore et toujours aux griffes du réseau social. Mais l'empire de Mark Zuckerberg ne cesse de s'étendre et touchera bientôt même ces irréductibles qui n'ont jamais ouvert de compte sur la plateforme.

L'entreprise a annoncé qu'elle allait diffuser des annonces à tous les visiteurs de sites utilisant sa régie publicitaire Facebook Audience Network, concurrente de Google Adsense. Autrement dit, même les personnes qui ne sont pas inscrites sur Facebook et celles qui n'y sont pas connectées seront ciblées par des publicités qui, jusqu'ici, n'étaient visibles que par les personnes connectées au réseau social.
Ce n'est un secret pour personne, la force de Facebook réside dans sa capacité à récolter des données sur ses utilisateurs. Grâce à cela, il peut facilement montrer des publicités ciblées et adaptées sur mesure en fonction des préférences identifiées. Une aubaine pour les annonceurs qui ne perdent ainsi pas de temps et d'effort à diffuser tous azimuthes leurs contenus.



TRAQUER LES HABITUDES DE TOUS LES INTERNAUTES
Mais comment Facebook peut-il en faire de même avec les personnes qui ne se trouvent pas dans son réseau ? Il va utiliser plusieurs outils à sa disposition pour traquer efficacement un maximum d'internautes, comme le fait Google. Facebook va ainsi se servir de cookies, de ses propres boutons et plugins de partage affichés sur les sites, ainsi que d'autres informations collectées sur les sites tiers.
« Nos boutons et nos plugins envoient des informations de base sur les sessions de navigation des utilisateurs. Pour les non-membres de Facebook, auparavant nous ne les utilisions pas. Maintenant nous allons les utiliser pour mieux comprendre comment cibler ces personnes », assume très clairement Andrew Bosworth, vice-président de Facebook en charge des publicités et de la plateforme commerciale.



Ce dispositif permettra à Facebook de repérer les habitudes des internautes en insérant des bouts de codes dans les cookies et dans les boutons ou autres contenus « embeddés », qui permettront d'identifier l'internaute, soit directement en tant que membre de Facebook, soit par un numéro unique qui lui sera attribué. Si vous visitez régulièrement un site de cuisine, Facebook affichera des publicités pour une cocotte-minute ou une friteuse sur les autres sites que vous fréquentez, en rémunérant le site qui les affiche.

QUELLE LÉGALITÉ EN EUROPE ?
Ce changement de politique de Facebook va certainement mécontenter une partie de la communauté des internautes, y compris chez les membres qui pourront continuer à être suivis même lorsqu'ils sont déconnectés du réseau social. Elle pourrait surtout déclencher les foudres des autorités si le système est déployé en Europe.
Lorsque la justice belge avait condamné Facebook à ne plus tracer les Belges non-membres de Facebook, le réseau social s'était fait fort de crier à l'injustice, en prétendant que son cookie (le DATR) avait pour seul intérêt de lutter contre le spam. « Nous utilisons le cookie datr depuis plus de 5 ans pour sécuriser Facebook pour 1,5 milliard de personnes à travers le monde », s'était agacé le réseau social. Or six mois plus tard, Facebook prouve que les autorités avaient raison de s'inquiéter.
En France aussi, la Cnil a demandé à Facebook de ne plus tracer les internautes qui ne sont pas inscrits et connectés sur le réseau social. Avec d'autres homologues, elle avait estimé que Facebook devait « se conformer à ce jugement (belge) sur tout le territoire de l'Union européenne ».
Selon la législation européenne, il est illégal de réaliser un traitement de données personnelles à des fins commerciales, sans le consentement explicite de la personne. Or si ce consentement peut être donné à l'inscription par Facebook, il ne peut certainement pas l'être par les non-membres… [Lire la suite]

Article de Omar Belkaab

Réagissez à cet article

Source : *Facebook vous traquera sur le Web même si vous n'êtes pas membre – Business – Numerama*

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

---

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

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]

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

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Arrêté en Belgique le 18 mars 2016 suite aux attentats de Paris du 13 novembre 2015, Monsieur Salah Abdeslam a été mis en examen notamment pour assassinats et tentatives d'assassinats en bande organisée en relation avec une entreprise terroriste, et placé en détention provisoire le 27 avril à la maison d'arrêt de Fleury Mérogis, dans l'attente de son jugement.

Il est aujourd'hui placé en isolement total dans une cellule de 9m2, et deux caméras le filment 24h/24. Cette mesure, tout-à-fait exceptionnelle, est justifiée, selon le Ministre de la Justice français, "conformément aux exigences la Convention Européenne de Sauvegarde des Droits de l'Homme et du droit français de la protection des données personnelles".
La loi française prévoit un régime dérogatoire s'agissant de la procédure pénale en matière de terrorisme, mais aucune disposition n'envisage spécifiquement la mise en place d'un dispositif de surveillance continue de la cellule d'un détenu. La Cour Suprême française (Cour de Cassation) a retenu à une reprise, en matière de criminalité organisée, la validité de la sonorisation permanente d'une cellule, sur autorisation du juge d'instruction.
Un arrêté français du 23 décembre 2014 autorise le contrôle sous vidéoprotection d'une cellule de protection d'urgence, mais ce texte ne vise que les détenus "dont l'état apparaît incompatible avec leur placement ou leur maintien en cellule ordinaire en raison d'un risque de passage à l'acte suicidaire imminent ou lors d'une crise aigüe" et alors la durée d'enregistrement ne peut dépasser 24 heures consécutives. C'est dans l'une de ces cellules de protection d'urgence pour les détenus suicidaires que monsieur Salah Abdeslam est actuellement détenu. L'arrêté ne serait donc applicable que s'il était démontré un risque imminent de passage à l'acte suicidaire, alors que Monsieur Salah Abdeslam est isolé, ses visites étant très limitées, et complètement isolé des autres détenus à chaque promenade. Il dispose en outre d'un pyjama en papier, sa cellule vide faisant l'objet d'une surveillance accrue par des rondes renforcées toutes les 3 heures. Monsieur Salah Abdeslam lui-même est encadré par une équipe de surveillants et médecins spécialisés dans les personnes dangereuses.
La Cour Européenne des Droits de l'Homme a permis aux détenus de bénéficier d'une véritable protection de leurs droits, en s'appuyant notamment sur l'article 3 de la convention, relatif aux traitements inhumains et dégradants. Les états membres doivent en effet s'assurer que la détention est compatible avec le respect de la dignité humaine et à veiller à ce que la santé et le bien-être du prisonnier soient assurés de manière adéquate. La Cour a déjà tenu compte, dans une affaire d'isolement carcéral et dans un contexte de la lutte contre le terrorisme, de la personnalité du détenu et de sa dangerosité hors norme, pour justifier de la mise en place de telles mesures (CEDH Grande Chambre, 4 juillet 2006, Ramirez Sanchez c/ France).
En matière de vidéosurveillance continue, la Cour Européenne a déjà été saisie de cette question, mais n'y a pas répondu, estimant que le requérant n'avait pas épuisé toutes les voies de recours internes dont il bénéficiait pour contester l'application de la mesure de sa vidéosurveillance (CEDH, Riina c/ Italie, 11 mars 2014). Le requérant, condamné à la réclusion à perpétuité pour association de malfaiteurs de type mafieux et de multiples assassinats se plaignait d'une vidéosurveillance constante dans sa cellule, y compris dans les toilettes.
Conscient de ce vide juridique, le Ministère de la Justice français a saisi l'autorité française de contrôle et de protection des données personnelles (CNIL), en charge notamment des questions liées la conservation des enregistrements et des mesures de vidéoprotection, d'un projet d'arrêté sur la vidéosurveillance en prison. Son avis sera rendu public dans les prochains jours.
En cas d'avis défavorable de la CNIL, l'avocat de Salah Abdeslam serait en droit de contester la mesure et de réclamer, outre une réduction de la mesure de vidéoprotection, une indemnisation financière devant le directeur de la prison, et en cas de rejet, de saisir le juge administratif français d'un recours. A charge pour l'avocat d'inscrire cette procédure de contestation dans une stratégie de défense plus générale… [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 : *Pourquoi la vidéosurveillance 24h/24 de Salah Abdeslam pose question légalement*

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*