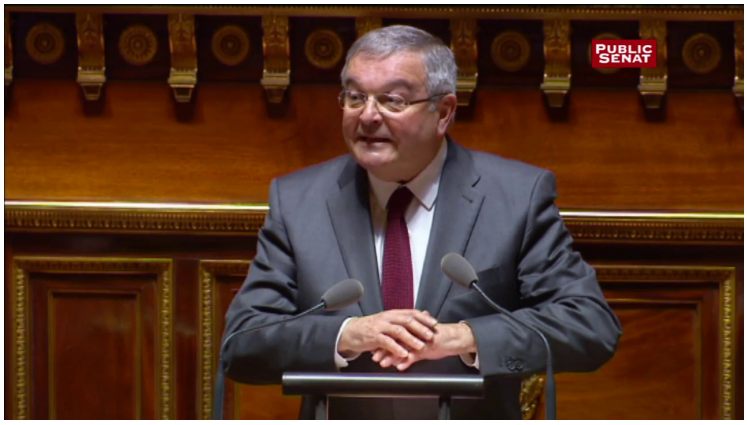
Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Quelles sont les limites d’accès aux données de connexion en situation d’État d’urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama

---

Facebook vous suit à la trace pour vous suggérer des amis

Facebook vous suit à la trace pour vous suggérer des amis

La géolocalisation de Facebook, utilisée notamment sur l'application mobile du réseau social, faisait déjà l'objet de nombreuses suspicions de la part des utilisateurs. Cette semaine, un porte-parole de Facebook a confirmé que la position géographique avait effectivement été utilisée par l'application pour suggérer de contacts que vous auriez pu croiser.

La fonction « Vous connaissez peut-être » de Facebook est souvent surprenante par sa précision, suggérant généralement des contacts pertinents. Si le site n'a jamais révélé vraiment les méthodes utilisées pour faire mouche aussi souvent, un de ses secrets vient en revanche d'être découvert : la géolocalisation permettrait de déterminer les personnes que vous fréquentez et qui disposent d'un compte. Concrètement, si deux personnes disposant d'un compte Facebook se trouvent au même endroit et ont activé la géolocalisation, le site proposera alors de les mettre en relation sur le réseau social.

« La localisation elle-même ne suffit pas à déterminer que deux personnes peuvent être amies », indique un porte-parole de Facebook au journal anglais The Telegraph. Et c'est justement un des arguments avancés par les détracteurs de cette fonction, qui y voient une atteinte à la vie privée. Le site n'étant pas capable de déterminer si deux personnes se trouvant au même endroit sont amies, ou même si elles se connaissent réellement, l'usage d'une telle fonction peut sembler abusif sur certains aspects, et poser quelques problèmes concernant l'anonymat que certains voudraient conserver en public. Facebook a cependant indiqué que cette fonction n'était aujourd'hui plus active sur son application mobile, et que celle-ci avait simplement fait l'objet d'un test limité. Les plus inquiets peuvent néanmoins désactiver la géolocalisation pour l'application.

Article original de Nicolas AGUILA

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

Original de l'article mis en page : Facebook vous suit à la trace pour vous suggérer des amis

Enquête sur l’algo le plus flippant de Facebook

Enquête sur l’algo le plus flippant de Facebook

Si la section « Vous connaissez peut-être » vous faisait parfois flipper en vous proposant des profils précis et éloignés de vos réseaux habituels, vous n'avez encore rien vu.
La section « Vous connaissez peut-être » (« People you may know ») de Facebook est une source inépuisable de spéculations. Cette fonction, en apparence sympathique puisqu'elle nous propose d'ajouter de nouveaux amis, semble détenir des informations très personnelles sur chacun d'entre nous.
• Une journaliste de la rédaction s'est ainsi vu proposer un flirt dont elle n'avait pas noté le téléphone dans son portable ;
• un autre collègue s'est vu proposer un pote qu'il n'a pas revu depuis 10 ans et qui venait de lui envoyer un mail ;
• une autre enfin, sa femme de ménage, dont elle a le numéro de téléphone dans son portable, mais avec laquelle elle n'a jamais eu aucune interaction en ligne.
Beaucoup ont aussi vu apparaitre des gens rencontrés sur des applis de rencontre comme Tinder ou Grindr. Plutôt embarrassant, non ?

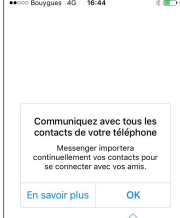
Folles rumeurs

Entre nous, les mots de « magie noire » et « espionnage » sont prononcés. Sur Internet, les rumeurs les plus folles circulent sur la façon dont cet algorithme plutôt intrusif fonctionnerait.
• Il existerait un « profil fantôme » de chacun d'entre nous, pré-rempli et automatiquement activé dès notre inscription.
C'est la théorie d'un utilisateur de Reddit. Il raconte avoir créé un profil anonyme avec un mail jamais utilisé et s'être vu proposer plein de contacts connus.
• A Rue89, on en formule une autre pour se faire peur : Facebook nous proposerait aussi les personnes qui nous « stalkent » (espionnent en ligne) ou que nous avons récemment « stalkées ».
Je découvre que cette rumeur existe déjà, et que beaucoup d'utilisateurs y croient dur comme fer. Facebook l'a toujours démentie.
• Dans le même genre, la sérieuse BBC affirmait, via des témoignages concordant et une société de sécurité informatique, que Facebook se connectait à des applications type Tinder ou Grindr pour vous faire des suggestions d'amis.
Un journaliste du Huffington Post a fait la même hypothèse. Ce que le réseau social a nié avec force.
Fabrice Epelboin, spécialiste des médias sociaux et entrepreneur du Web, croit les dires de Facebook, comme Vincent Glad :
« Ce serait très dangereux économiquement. Facebook n'est pas une société idiote, elle prend des risques calculés. »
Pour lui, l'explication est beaucoup plus simple :
« Quand on "date" quelqu'un sur Tinder, on lui donne bien son numéro avant, non ? Facebook se connecte en fait à votre répertoire. »
Ah bon ?

Un aspirateur à données, via votre téléphone

On résume. Il faut imaginer l'algorithme de Facebook comme un aspirateur à données géant.

*Visages et Facebook — **Pixabay/CC0***
*Dans un article du Washington Post, qui fait référence en la matière, il **est expliqué** que l'algorithme de « Vous connaissez peut-être » est basé sur la « science des réseaux ».*
En définissant les réseaux auxquels on appartient, Facebook calcule nos chances de connaître telle ou telle personne. Et il peut même prédire nos futures amitiés. Un peu de probabilités et c'est dans la boîte.
« Ce n'est pas de la magie, mais juste des mathématiques très pointues », apprend-on.



Avertissement de Messenger, dont la « synchronisation » permet au contact de « se connecter sur Facebook »
*En fonction des amis que l'on a, de nos interactions plus ou moins fortes et fréquentes avec eux, de l'endroit où on vit, des lieux où on a étudié et travaillé, l'algorithme fait ses calculs. Il tente aussi de définir les personnes « clés » de votre réseau, celles qui vous présentent aux autres. Enfin, il utilise votre géolocalisation, ce qui a **probablement mené** ce lundi à l'arrestation du voleur de la voiture d'un internaute, qui est apparu dans ses suggestions d'amis.*
Surtout, depuis qu'il est arrivé sur votre mobile, via les applis Facebook et Messenger, le réseau social a un tas d'autres informations à mettre sous la dent de leur algo : vos contacts téléphoniques et vos mails.
Vous l'avez autorisé, probablement sans en avoir conscience, au moment de l'installation de l'une et/ou l'autre application.

Le test ultime : le Nokia de Xavier de La Porte

Comme c'était un jour de pluie, j'ai voulu tester la puissance de cet algorithme qui marche donc sur deux pieds :
• La « science des réseaux » ;
• des tonnes de données « scrapées » de notre mobile notamment.
Je décide de créer un compte avec un numéro de téléphone et avec un faux nom. Le mien est déjà lié à un compte, donc Facebook le refuse.
*En effet, il est interdit, en théorie, de créer un faux compte ou de doublonner, selon sa politique de « l'identité réelle » — les personnes transgenres en **savent** malheureusement quelque chose.*
Il y a une personne dans ces bureaux qui n'a pas lié son compte Facebook à son numéro. J'ai nommé : Xavier de La Porte. Il possède un charmant Nokia cassé sur le dessus.

Le téléphone de Xavier, bolide de la protection des données
« J'ai 20 contacts dessus, seulement ma famille et mes amis proches », jure-t-il.
Il n'est évidemment pas question d'applications quelconques. Avec le numéro de Xavier, Facebook accepte la création du compte de « Mathilde Machin », 21 ans.

« Mathilde Machin », couverture très discrète
Et là, un truc vraiment effrayant arrive : des dizaines de contacts sont proposés, amis, famille, collègues de bureau, sources de Xavier. Ils ne sont pas dans son répertoire. Et ne sont pas non plus tous amis avec lui sur Facebook. A partir de là, deux hypothèses s'offrent à moi :
• Son compte a été lié un jour à ce numéro de téléphone, et Facebook se rend compte qu'il s'agit de la même personne. Il lui propose logiquement d'ajouter les amis du compte de Xavier.
Mais, Facebook refuse d'ouvrir deux comptes avec le même mail ou le même numéro. Il s'agirait d'une sorte de faille de sécurité, puisque le téléphone sert justement à sécuriser votre compte. Et cela n'expliquerait pas pourquoi Mathilde Machin se voit proposer des personnes qui ne sont pas dans les amis Facebook de Xavier.
• Les contacts proposés sont ceux qui possèdent le numéro de Xavier dans leur répertoire. Et qui ont donné à Facebook l'autorisation de scraper leurs données. Ce qui veut dire que l'algorithme de suggestion est tellement puissant qu'il réussit, en quelques secondes, à « inverser » la recherche.
Facebook, après s'être creusé les méninges un moment — c'est un peu technique —, me confirme la dernière hypothèse.
*C'est vertigineux. Mais inscrit noir sur blanc dans les flippantes« **Confidentialités et conditions** » de Facebook. Qui autorisent l'application à utiliser les « données que vous importez ou synchronisez de votre appareil », type répertoire, mais aussi :*
*« Les contenus et informations que **les autres personnes** fournissent lorsqu'elles ont recours à nos services notamment des informations vous concernant, par exemple **lorsqu'elles partagent une photo de vous, vous envoient un message ou encore lorsqu'elles téléchargent, synchronisent ou importent vos coordonnées.** »*

Un algo gourmand

Facebook m'explique donc que l'algorithme se nourrit aussi des données que les autres ont sur vous (votre mail, votre numéro). Pour le dire autrement, quelqu'un qui a votre contact et l'importe dans son appli Facebook va probablement apparaître dans vos suggestions d'amis. C'est aussi fou que les rumeurs. Facebook insiste sur le fait que :
• Le processus est transparent ;
• l'algorithme, gentil, ne cherche qu'à vous faire retrouver vos amis et échanger avec eux ;
• « Facebook ne possède pas et n'utilise pas » votre numéro de téléphone, il s'en sert pour mettre en relation des profils ;
• et les paramètres de votre compte sont personnalisables.
Un samedi soir, vous êtes tombée amoureuse d'un ami d'ami. Le lendemain, vous demandez à l'ami commun son numéro. Vous hésitez à envoyer un message, vous bloquez plusieurs jours. Sachez donc que ce mec, à qui vous n'avez rien envoyé, vous a peut-être déjà vu apparaître dans « Vous connaissez peut-être ». Et qu'il a déjà peur de vous.
Article original de Alice Maruani Rue 89

Réagissez à cet article

Original de l’article mis en page : Enquête sur l’algo le plus flippant de Facebook – Rue89 – L’Obs

---

Facebook regarde dans quels magasins vous faites vos courses

Facebook regarde dans quels magasins vous faites vos courses

Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.

Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d'un carrousel – pour indiquer à l'internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s'inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d'afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s'y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l'occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu'environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n'a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n'est d'ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Moutain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l'utilisateur et de sa géolocalisation.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

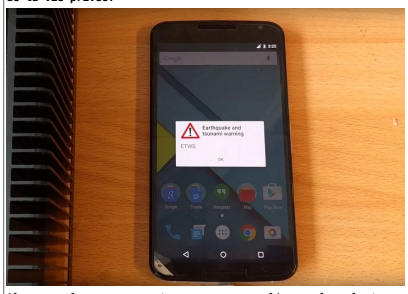
---

Appli alerte attentats : «Il

faut que la France respecte les standards internationaux»

	**Application Alerte Attentats : «Il faut que la France respecte les stahdards internationaux»**

Alors que le gouvernement propose une application pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.



Alors que le gouvernement propose une appli pour les alertes aux attentats, Gaël Musquet, hacker et militant du logiciel libre, presse l'Etat d'adopter la diffusion cellulaire, plus efficace et respectueuse de la vie privée.
Le gouvernement a dévoilé mercredi une application, «SAIP» (pour «Système d'alerte et d'information des populations»), permettant d'alerter en direct ses utilisateurs en cas d'attentat à proximité. Une bonne initiative, mais une réponse technologique inappropriée, estime Gaël Musquet, hacker en résidence à la Fonderie, l'Agence numérique publique d'Ile-de-France. Car des normes internationales existent déjà pour transmettre une alerte sur tous les téléphones des populations menacées par un risque, sans qu'elles aient besoin d'installer une application, et en respectant leur vie privée.

Que penser de cette application d'alerte gouvernementale ?
Prévoir un protocole d'alerte aux populations est une bonne initiative, on va dans le bon sens. Nous n'avons pas une grande culture du risque en France, donc toutes les occasions d'en parler sont bonnes à prendre ! Cela permet de faire de la pédagogie, d'informer et de former les populations. Car c'est le manque de préparation qui crée de la panique, et malheureusement, parfois des morts. Et puis franchement, les sirènes d'alerte ne sont comprises par personne, donc il est temps de rafraîchir le système avec un peu de technologie.
Le taux d'équipement en smartphones permet aujourd'hui de toucher un maximum de personnes quand on développe une application sur les deux principales plateformes, iOS et Android. Le gouvernement a eu une démarche d'ouverture, en consultant par exemple Visov, une association de volontaires spécialistes de la gestion d'urgence – ils font de la pédagogie auprès des pompiers, des gendarmes ou de l'Etat, entre autres, sur l'utilisation du Web et des réseaux sociaux en cas de crise. Le développement de SAIP est encore en cours, et il appartient au Service d'information du gouvernement [SIG] de recueillir les premiers retours pour améliorer le service. Il a fait cette application de la manière la plus agile possible, on ne peut pas lui faire de reproche là-dessus.

Mais… ?
Il y a plusieurs problèmes avec cette démarche. D'abord, l'application SAIP s'appuie sur les données internet des smartphones, donc sur les réseaux 3G, 4G et wifi qui sont potentiellement vulnérables. Quand il y a trop de téléphones dans une certaine zone et pas assez de canaux disponibles pour pouvoir router tous les appels, les antennes-relais sont saturées et elles ne peuvent plus répondre. Ça se passe régulièrement dans les événements où il y a foule : pendant les attentats de Boston, au discours d'investiture d'Obama mais aussi le 13 Novembre, il y a eu ce qu'on appelle un Mass Call Event (MCE). C'est aussi le cas localement dans des quartiers à cause de concerts, festivals… Quand on sait à l'avance qu'il y aura trop d'appels durant un événement, on installe des antennes-relais supplémentaires pour couvrir le risque de saturation. C'est ce qui va se passer pour l'Euro de foot. Mais en cas de crise imprévue, les infrastructures ne résisteront pas, ni pour les appels, ni pour les SMS, ni pour les données internet. Ce sont des lois physiques, on ne peut rien y faire. Dans ce genre de situation, SAIP sera dans les choux.
Ensuite, il faut faire attention à ne pas morceler le système d'alerte avec de multiples applications de gestion de crise. Il existe une appli pour le risque d'attentats en France, une pour les séismes du Centre sismologique euroméditerranéen, une autre pour mes vacances en Russie et une pour les alertes de l'Indre-et-Loire… Il y a aussi des entreprises privées qui développent leurs propres applications d'alerte, et des fois, comme pour les risques d'avalanches, elles sont meilleures que celles de l'Etat. La concurrence entre les acteurs est contre-productive pour toucher un maximum de personnes. Il vaut mieux un système universel qui puisse aussi s'adresser, par ailleurs, aux touristes de passage en France.
Enfin, il y a la question du respect de la vie privée. Beaucoup d'internautes s'inquiètent déjà, sur Twitter, que l'Etat puisse savoir en permanence où je me trouve via les données de géolocalisation récoltées par cette application. Et il existe effectivement un risque que ces données soient piratées, quels que soient les efforts de sécurisation. Et puis, comme ce n'est pas un logiciel libre, on ne connaît pas son code source et la communauté des développeurs ne peut pas aider à corriger les bugs, faire des stress tests pour vérifier son fonctionnement dans des conditions d'usage intense…

Y a-t-il une meilleure solution ?
A court terme, c'est bien d'avoir une application d'alerte. Mais à long terme, on n'y coupera pas : il faut que la France respecte les standards internationaux de la diffusion cellulaire – cell broadcast en anglais. C'est une norme qui existe déjà pour la diffusion des alertes, et qui permet d'informer toutes les personnes présentes dans la zone de couverture d'une antenne-relais. On n'a pas besoin de connaître leur numéro de téléphone ni de leur faire installer une application : dans la région prédéfinie, tout le monde sans exception reçoit le SMS, y compris les touristes avec un forfait étranger ! C'est une technologie non intrusive qui respecte la vie privée des citoyens. Elle ne se limite pas aux possesseurs d'iPhone et d'Android, même pas besoin d'avoir un smartphone : l'alerte arrive même sur les petits téléphones. Ça tombe bien : en France, 92 % des personnes de plus de 12 ans ont un téléphone, mais 58 % seulement ont un smartphone. Et puis la norme cell broadcast prévoit que les messages d'alerte passent au-dessus de la mêlée dans le trafic téléphonique.

Simulation d'une alerte en diffusion cellulaire sur Android.

La norme du cell broadcast est définie depuis 1995 (pdf et pdf). Elle a même été testée à Paris en 1997 : tout est déjà là ! Depuis, elle a évolué pour supporter les alertes enlèvement (Amber), les séismes et les tsunamis (système ETWS). Avec l'arrivée de la 4G, le protocole a encore été étendu et on peut même l'utiliser pour diffuser des vidéos, aujourd'hui. Vingt ans plus tard, la diffusion cellulaire a été déployée par nos voisins – Espagne, Portugal, Italie, Finlande, Pays-Bas, Chine, Etats-Unis, Israël… Et la France brille par son absence.
Nous devons, nous aussi, la mettre en place dans le cadre d'une véritable politique numérique de l'alerte. Il y a là un enjeu de sécurité publique. Cette norme doit être imposée à nos opérateurs téléphoniques, comme un service public de l'alerte, comme on a imposé la mise en place du 112. C'est une question d'intérêt général. Pourquoi ne respectons-nous pas les normes et standards internationaux en matière d'alerte, documentés, ouverts et qui ont fait leurs preuves ?

Pourquoi n'a-t-on pas encore déployé la diffusion cellulaire en France ?
C'est fragile et ça coûte cher, nous dit-on. Oui, ça coûte cher, mais pas plus que la Hadopi ! On a su débloquer des budgets pour les lobbys de l'industrie culturelle et créer, entretenir, maintenir l'Hadopi à grands frais en contraignant les opérateurs à suivre. Idem pour l'espionnage de masse avec les lois sur la surveillance. Si tu es capable de m'espionner, alors tu es capable de m'informer en cas de crise. Est-ce que notre sécurité vaut moins que les doléances d'autres lobbys ? Nos vies sont-elles moins chères que la Hadopi ?
La mise en place du cell broadcast demande effectivement, quoique pas obligatoirement, de légiférer. Ça demande ensuite que les systèmes d'information des préfectures soient reliés aux systèmes d'information des opérateurs téléphoniques : il faut des passerelles pour que l'alerte passe de la préfecture à SFR, Bouygues et compagnie. Ça demande de la réflexion et un chantier technique. A part ça, c'est simple : les antennes-relais respectent déjà la norme.

Simulation d'une alerte en diffusion cellulaire sur iPhone.

Il faut juste activer l'option. Nos voisins chiliens ont su le faire pour se protéger des tsunamis ; en septembre 2015, il leur a fallu quelques dizaines de minutes seulement pour évacuer des milliers de personnes après le séisme. Il n'y a pas de raison que la France n'y arrive pas aussi !

C'est une question plus générale de culture du risque…
L'alerte est une chose, oui, mais ce n'est pas suffisant. La France est un pays qui fait face à tous les risques possibles, mais nous n'avons pas de culture du risque. Alors que les risques, eux, sont bien là. Notre mémoire est courte mais nous avons des catastrophes naturelles bien plus meurtrières que le terrorisme : 500 morts après la rupture du barrage de Malpasset en 1959, 46 morts avec le séisme provençal de 1909, 29 000 morts pour l'éruption en 1902 de la Montagne Pelée, 70 000 morts dans le tsunami de 1908 à Messine, et même 29 morts récemment à La Faute-sur-Mer et 17 morts dans les inondations de la Côte d'Azur en octobre 2015.
Il faut faire des exercices : un barrage a lâché, que fait-on ensuite ? Les gens paniquent quand ils ne savent pas quoi faire, on l'a encore vu la semaine dernière avec les crues. Il faut des exercices communaux pour expliquer les procédures aux habitants des villes, former des gens à l'utilisation des réseaux sociaux en cas d'urgence pour contrer les rumeurs et diffuser les informations, former des pilotes de drones et des radioamateurs : le jour où il y a un vrai black-out de téléphonie, qui saura faire la transmission des informations ? Au-delà d'événements très médiatiques comme les hackathons ou les simulations entre experts, nous devons impliquer la société civile dans des exercices réguliers.
Commençons à expérimenter sur des territoires français de petite taille, en proie à des crises cycliques – Guadeloupe, Martinique, Réunion, Polynésie… Des formats d'événements existent déjà. CaribeWave, IndianWave et PacificWave sont par exemple des exercices annuels d'alerte au tsunami, auxquels je participe. Les Etats-Unis organisent un «préparathon» contre les catastrophes naturelles.

2016 est l'année de la présidence française de l'Open Governement Partnership. Pour un gouvernement ouvert, à nous, société civile, de nous prendre en charge, nous investir dans les exercices et les réflexions pour une meilleure information et une meilleure préparation aux crises.
Vendredi après-midi, tout le matériel technologique ayant servi à CaribeWaveFWI, la dernière simulation d'alerte au tsunami, sera exposé à la Gaîté Lyrique à Paris, dans le cadre du festival Futurs en Seine.

Article original de Camille Gévaudan

Réagissez à cet article

Original de l’article mis en page : Appli alerte attentats : «Il faut que la France respecte les standards internationaux» – Libération

---

Deux applications accusées d’espionner les coureurs

Deux applications accusées d’espionner les coureurs

Les applications Runkeeper et Tinder viennent d'être dénoncées par le conseil des consommateurs norvégien. En effet, elles exploiteraient illégalement les données des utilisateurs.

Si vous ne le savez pas encore, Runkeeper est une application qui permet de mesurer ses performances sportives. Si on parle d'elle aujourd'hui, ce n'est pas vraiment pour les fonctionnalités qu'elles proposent, mais plutôt pour un sujet plus serré. En effet, cette application qui est la possession de la société FitnessKeeper violerait les règles de confidentialité des données personnelles. D'après le NCC (conseil des consommateurs norvégien), afin de pouvoir évaluer l'état de l'utilisateur, elle doit d'abord accéder à des fonctionnalités stratégiques telles que la géolocalisation.
Et le comble dans tout cela, c'est le fait que les données de l'utilisateur ayant été collectées seraient ensuite utilisées pour des finalités commerciales. En effet, elles seraient revendues à des entreprises de publicité et seraient même sauvegardées même après la suppression du compte. En tout cas, c'est ce qu'avance un rapport qui date du 10 mai. Interrogé sur cette question, le fondateur de Runkeeper a indiqué que le problème vient d'un bug. « Nous sommes en train de sortir une nouvelle version de notre application qui élimine ce bug… Nous prenons au sérieux la confidentialité des données des utilisateurs… », a-t-il indiqué. Par ailleurs, outre l'application Runkeeper, le NCC pointe aussi du doigt l'application Tinder, laquelle est une application pour les fans de rencontre amoureuse. Elle, aussi, conserverait les données des utilisateurs, notamment, les photos et les conversations… [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.

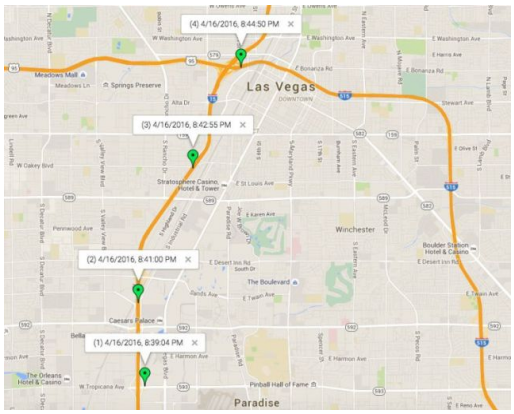
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Runkeeper et Tinder : les deux applications accusées d'espionner les coureurs – MeilleurActu*

Waze : les hackeurs peuvent vous suivre à la trace

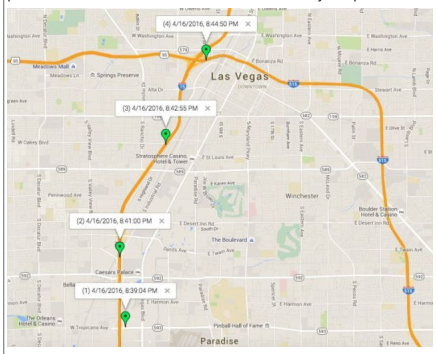


Waze : les hackeurs peuvent vous suivre à la trace

Des experts en sécurité informatique ont découvert une faille permettant d'espionner en temps réel les trajets des utilisateurs de l'application de navigation communautaire Waze. Selon eux, presque toutes les applications d'aide à la conduite seraient concernées. Explications.

C'est l'une des applications d'aide à la conduite les plus populaires en France. Aujourd'hui, près de 5 millions d'automobilistes utilisent presque quotidiennement le service de navigation communautaire Waze. Il a y a quelque mois, des chercheurs de l'Université de Californie à Santa-Barbara (Etats-Unis) ont découvert une faille, partiellement corrigée seulement, qui permet à des hackeurs d'espionner en temps réel les déplacements de n'importe quel utilisateur.
L'équipe d'experts en sécurité informatique a suivi durant trois jours les trajets d'une journaliste du site américain Fusion. Afin de vous livrer les informations de trafic, Waze utilise une connexion sécurisée pour communiquer avec votre smartphone. Or c'est justement là que se trouve la faille. Les chercheurs sont parvenus, en effet, à se placer entre les serveurs de l'application et l'utilisateur. De ce fait, ils ont pu intercepter toutes ses données de navigation, ainsi que ses trajets en bus ou en taxi.

Voiture fantôme, véhicule espion, embouteillage virtuel
Une fois infiltrés dans les serveurs de l'application, ils ont pu étudier en détail le fonctionnement des algorithmes de Waze. Au-delà des problèmes de confidentialité, les chercheurs se sont aperçus qu'ils pouvaient également créer des véhicules « fantômes ». Dans le but, par exemple, de créer de faux embouteillages ou d'épier tous les utilisateurs se trouvant à proximité de ce conducteur virtuel. En envoyant plusieurs véhicules fantômes, ils affirment avoir été en mesure de quadriller un quartier entier.



D'après ces experts en sécurité en informatique, il serait même possible de surveiller l'intégralité de la population américaine, simplement "en utilisant quelques serveurs de plus". Imaginez : tous vos trajets pourraient être enregistrés et mis à disposition du plus offrant. L'équipe de recherche a informé Waze de sa découverte, il y a plusieurs mois, et l'application, rachetée par Google en 2013, avait procédé à une mise à jour. Mais elle ne corrige que partiellement la faille.
« Toutes ont quasiment toutes ce type de failles »
Depuis janvier dernier, les données de géolocalisation ne sont plus partagées avec les conducteurs situés à proximité lorsque l'application est ouverte en tâche de fond. En revanche, il est toujours possible de vous espionner lorsqu'elle est en marche. Mais la faille est toujours présente quand on l'utilise en premier plan.

Comment faire ? ⇒ Seule solution pour le moment : utiliser le mode invisible… qui se désactive automatiquement à chaque redémarrage de l'application.

Waze semble être en effet conscient de ses lacunes. Dernièrement, l'application a mis en place une fonction censée permettre à son utilisateur de masquer son emplacement réel. Cependant, comme on le démontre l'enquête de Fusion, ce nouveau système n'est pas vraiment efficace. Et surtout, elle n'est pas à la seule application concernée, si l'on en croit Ben Zhao : « Nous avons étudié de nombreuses applications. Presque toutes ont ce type de failles. Nous ne savons pas comment stopper cela », s'inquiète Zhao. Pas de quoi rassurer les automobilistes… [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (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

Suivez-nous sur

Réagissez à cet article

Source : *Waze : les hackeurs peuvent vous suivre à la trace – metronews*

Mieux connaître le consommateur avec ses données

Mieux connaître le consommateur avec l'analyse prédictive et le Big Data

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients.

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients. Habitudes d'achat, fréquence et lieux des visites, horaires… Toutes ces informations forment une base de données gigantesque et sans cesse en mouvement. C'est ce que l'on nomme « Big Data » et il s'agit d'une véritable mine d'or pour les professionnels du marketing. Fini les suppositions logiques et autres préjugés, l'analyse prédictive permet maintenant de dégager des statistiques et schémas de consommation concrets.

D'où viennent les informations qui composent le Big Data ?

Chaque fois que vous activez votre géolocalisation en consultant un site internet ou une application, cela laisse une trace. Les données du Big Data sont également composées par vos habitudes de navigation sur le net, les endroits où vous vous rendez, combien de temps vous restez, d'où vous venez, ce que vous regardez… Bien sûr toutes ces informations sont rendues anonymes, mais vos terminaux, dont votre smartphone, sont de véritables espions dans votre poche. Un data scientist, tels que sont nommés les experts du Big Data, s'intéressera aux patterns et croisera vos données avec celles de milliers d'autres personnes. Il s'agira par exemple de créer des algorithmes adaptés aux habitudes de navigation des utilisateurs d'un moteur de recherche. L'idée est d'aller chercher dans les données des tendances, et d'identifier des comportements. Analyser, comprendre… puis prédire les actions futures. Cela est désormais possible et relativement simple avec les outils dont disposent les analystes.

Le Big Data, un outil d'analyse prédictive qu'il faut savoir exploiter

Si le Big Data peut servir à améliorer l'expérience des utilisateurs d'un produit, il révèle surtout son potentiel dans le secteur du marketing. Grâce à l'analyse du flot des données, il est possible d'établir des segments toujours plus pertinents. Finie la publicité « à destination de la ménagère de 40 ans ». Vous êtes désormais en mesure de savoir qui est réellement susceptible d'utiliser vos produits, et avec quel argument mettre en avant votre offre. Bien sûr, cela demande un réel travail d'analyse et ce n'est pas un hasard si vous voyez fleurir les offres d'emploi de data scientist ou de data mining. Le marketing et l'analyse prédictive deviennent des travaux de statisticien. Cela demande également de disposer des bons outils. Il s'agit d'un investissement en plusieurs étapes :

1. Vous collectez les données transmises par toutes les sources pertinentes ;
2. Vous analysez les données et isolez les schémas de consommation qui vous intéressent. L'étude de leurs occurrences sera la base de vos analyses prédictives ;
3. Enfin, vous établissez une stratégie de marketing ciblée en fonction des résultats obtenus.

Pour une efficacité maximale, la majeure partie de ce processus sera automatisée. Pour gagner en efficacité mais aussi en efficience grâce à des outils de traitement des données en temps réel, il est possible de créer des processus semi-automatisés. L'intervention humaine n'est plus utile ? C'est le contraire. Elle est essentielle. L'œil humain est là pour aller chercher dans les données, fouiner et faire émerger des signaux faibles. La technologie libère le potentiel des données, mais il faut une intervention humaine pour bien utiliser ces outils, et en tirer des décisions actionnables.

Comment se servir de l'analyse prédictive pour optimiser son ROI ?

S'il peut être intéressant d'analyser le Big Data pour de multiples raisons, en matière de marketing l'objectif est avant tout d'améliorer votre ROI (Return On Investment). Pour cela, votre démarche analytique doit s'inscrire dans un plan d'action concret.
Que vous soyez spécialisé dans le e-commerce ou que vous réalisiez toutes vos ventes dans des magasins physiques, utilisez les données pour améliorer votre marketing digital.

Lancez des campagnes de marketing ciblées ;

Démarquez-vous du flot de publicité, et adaptez votre proposition aux envies réellement exprimées de vos clients.
Mais l'analyse prédictive ne sert pas qu'à générer des ventes. Elle trouve aussi son utilité dans le maintien de la relation client. Il est par exemple possible de déterminer quand un client est sur le point de résilier un abonnement, quand celui-ci est sur le point de basculer chez un concurrent… pour pouvoir le retenir ! A l'aide de ces informations contenues dans votre Big Data, vous pouvez améliorer votre taux de fidélité en adaptant vos offres au bon moment. Un exemple ? La chaîne d'hôtel Hyatt utilise désormais l'analyse prédictive pour donner à son personnel d'accueil des informations supplémentaires sur les clients. En analysant la recherche menée par ces derniers sur le site et les applications du groupe, Hyatt précise si un client peut être intéressé par une chambre avec vue (car il a regardé plusieurs fois la page) ou s'il désire peut-être une chambre avec des oreillers anallergiques, car il a tapé ce mot clé dans le moteur de recherche interne… Un bel exemple de personnalisation de la relation client, grâce aux données.M… [Lire la suite]

Suivez nous sur

Réagissez à cet article

Source : *Analyse prédictive et Big Data : mieux connaître le consommateur avec ses données*

Un piratage sur Tor par le FBI prive les victimes d'une justice

Un piratage sur Tor par le FBI prive les victimes d'une justice

---

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

CNIL, un nombre record de plaintes en 2015

CNIL, un nombre record de plaintes en 2015

L'année 2015 est marquée par une forte augmentation de l'activité de la CNIL, avec 13 790 demandes provenant de particuliers : 7908 plaintes dont 36% concernent l'e-réputation et 5 890 demandes de droit d'accès indirect. Cette évolution témoigne de la volonté des citoyens de reprendre leurs droits en main au bénéfice de plus de transparence et de sécurité, notamment dans la gestion de leur e-réputation.

Protéger sa vie privée en ligne : de la préoccupation à la responsabilisation

En 2015, la CNIL a enregistré 7 908 plaintes, soit 2000 de plus qu'en 2014 (36 % de hausse).

Cette augmentation importante s'explique par la prise de conscience croissante des citoyens, notamment pour la gestion de leur réputation en ligne. Cela se traduit par la pratique régulière de l'ego-surfing, qui est souvent à l'origine de demandes de retraits de contenus ou de déréférencement. En cas de refus de l'éditeur du site ou du moteur de recherche, la CNIL peut être saisie d'une plainte. A titre indicatif, la CNIL a ainsi reçu près de 700 plaintes depuis l'été 2014 et la consécration par la Cour de justice de l'Union européenne d'un droit au déréférencement. Enfin, la médiatisation d'affaires touchant à la sécurité des données tend aussi à sensibiliser les citoyens à cette problématique croissante.

L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes, ainsi que l'exercice du droit d'accès.

Afin de faciliter les démarches des personnes qui la saisissent et de fiabiliser leurs demandes, la CNIL a amélioré en avril 2015 son service de plaintes en ligne en déployant une cinquantaine de scénarios correspondant aux plaintes les plus fréquentes.

C'est nouveau ! A suivre …

Les plaintes reçues permettent à la CNIL d'identifier de nouvelles tendances telles que : la géolocalisation des salariés non plus via leur véhicule mais via des bracelets connectés ou leur smartphone, de nouvelles techniques de vidéosurveillance des salariés via une application sur smartphones ou une webcam.

Des municipalités invitent leurs administrés à leur envoyer des photos ou du son pour signaler des incivilités (déjections canines, stationnement abusif, tapage nocturne, dépôt d'ordure, affichage sauvage, etc).

Des demandes de droit d'accès indirect toujours en hausse

En 2015, la CNIL a reçu 5890 demandes de droit d'accès indirect, soit une augmentation de 12% par rapport à 2014. Ces demandes reçues représentent un total de 8377 vérifications à mener concernant par ordre d'importance : le fichier FICOBA de l'administration fiscale, le fichier TAJ des antécédents judiciaires de la police et de la gendarmerie et les fichiers de renseignement.

Les effets des attentats et de l'état d'urgence sur les demandes de droit d'accès indirect

La CNIL a reçu ces derniers mois près de 155 demandes de droit d'accès indirect liées au contexte de l'état d'urgence (perquisitions administratives, assignations à résidence, retrait de badges aéroportuaires ou de cartes professionnelles). Ces demandes portent notamment sur le Traitement d'Antécédents Judiciaires (TAJ) et les fichiers des services de renseignement du ministère de l'intérieur.

Le renforcement des effectifs au sein des forces de sécurité depuis les attentats du 13 novembre 2015 (création annoncée de 8500 postes dans la police, la gendarmerie, la douane et l'administration pénitentiaire) et l'accroissement du nombre de candidats à ces fonctions contribuent également à accroître le nombre demandes de droit d'accès indirect au fichier TAJ, consulté dans le cadre des enquêtes administratives menées pour l'accès à ce type d'emplois.

Au premier trimestre 2016, la CNIL a déjà constaté une augmentation de 18 % des demandes d'accès au fichier TAJ par rapport au premier trimestre 2015.

Une action répressive en hausse, notamment grâce aux contrôles en ligne

La logique de la loi et son application par la CNIL visent avant tout la mise en conformité des organismes mis en cause. A chaque phase d'instruction d'une plainte et/ou d'un contrôle, ceux-ci ont la possibilité de suivre les mesures recommandées par la CNIL pour se mettre en conformité. **Dans l'immense majorité des cas, la simple intervention de la CNIL se traduit par une mise en conformité de l'organisme**. Le prononcé de sanctions par la CNIL permet de sanctionner des organismes qui persistent dans des comportements répréhensibles, et constitue donc un instrument de dissuasion important.

L'année 2015 se caractérise par une forte augmentation du nombre de mises en demeure adoptées par la Présidente de la CNIL. **En effet, 93 mises en demeure** ont été adoptées contre 62 en 2014.

Cette hausse s'explique par la possibilité de réaliser des contrôles en ligne et par le fait que des contrôles s'inscrivaient dans des thématiques ayant révélé de nombreux manquements :

- cookies (40 mise en demeure),
- sites de rencontre (8 mise en demeure),
- services dématérialisés d'actes d'état civil (20 mise en demeure).

10 sanctions ont été prononcées par la formation restreinte, dont 3 sanctions pécuniaires.

La CNIL a réalisé **501 contrôles** en 2015, dont **87 contrôles portant sur des dispositifs vidéo**.

155 contrôles en ligne ont été réalisés sur de nombreuses thématiques telles que :

- les sites de tirage de photos ou de créations d'albums photo,
- de conseil de santé en ligne,
- de crédit en ligne,
- d'adhésion à des partis politiques,
- de demande d'actes d'état civil,

28 contrôles en ligne réalisés en 2015 ont conduit à une mise en demeure en 2015, 2 procédures de sanction ont été engagées et toujours en cours.

Les données personnelles, au cœur de l'actualité législative en France et en Europe

En 2015, l'actualité législative s'est fortement structurée autour de la protection des données personnelles et des libertés numériques, comme en témoignent les 122 avis que la CNIL a rendus.

Le renseignement et la lutte contre le terrorisme

La CNIL s'est prononcée sur **14 projets de dispositions législatives ou réglementaires directement relatives au traitement de données à des fins de renseignement ou de lutte contre le terrorisme**. Des dispositifs d'une nouvelle ampleur, en termes de volume de données traitées comme de modalités de collecte, ont été légalisés. De nouveaux fichiers ont été créés, certains fichiers existants ont été modifiés, de nouvelles techniques d'enquête et de recueil de données ont été utilisées pour surveiller et contrôler des communications.

Une personnalité qualifiée au sein de la CNIL est chargée depuis février 2015 de contrôler le blocage administratif des sites provoquant des actes de terrorisme ou en faisant l'apologie ainsi que les sites à caractère pédopornographique. Ce contrôle vise à s'assurer que le blocage n'est pas disproportionné afin d'éviter tout « sur blocage ». Alexandre Linden, la personnalité qualifiée désignée par les membres de la CNIL, présentera un rapport dédié à cette activité.

Dans le cadre du projet de loi relatif au renseignement, la CNIL a rendu un avis le 5 mars 2015, dans lequel elle a été très attentive aux modalités de contrôle des fichiers de renseignement. Ces fichiers bénéficient actuellement d'un cadre législatif spécifique interdisant le contrôle de leur régularité du point de vue de la loi Informatique et Libertés. Or, un tel contrôle général constitue une exigence fondamentale afin d'asseoir la légitimité démocratique de ces fichiers dans le respect des droits et libertés des citoyens.

La CNIL a proposé que le projet de loi lui permette d'exercer un tel contrôle, selon des modalités particulières, adaptées aux activités des services de renseignement, et en coopération avec la CNCTR (Commission Nationale de Contrôle des Techniques de Renseignement). Cette proposition n'a pas été suivie d'effet.

Le projet de loi pour une République numérique conforte et renforce l'action de la CNIL

La CNIL s'est prononcée, lors de la séance plénière du 19 novembre 2015, sur l'avant projet de loi pour une « République numérique », dans sa version alors envisagée par le Gouvernement. Le projet de texte adopté en première lecture à l'Assemblée nationale comporte de nombreuses modifications, qui tiennent notamment compte de l'avis de la CNIL. La CNIL a insisté dans son avis sur la nécessaire cohérence avec les autres textes en préparation et particulièrement le règlement européen qui sera d'application directe en 2018.

Le projet de loi tend également à renforcer les pouvoirs de la CNIL et à conforter ainsi son engagement dans la régulation du numérique et son activité d'accompagnement des particuliers, des entreprises et des administrations.

La loi du 26 janvier 2016 sur la modernisation de notre système de santé

La CNIL a été sollicitée sur le projet de loi et a participé à de nombreuses auditions.

En Europe

Au plan international, la finalisation du projet de règlement européen sur les données personnelles qui a fait l'objet d'un accord à l'issue du trilogue en décembre 2015 et l'arrêt de la CJUE d'octobre 2015 invalidant le Safe Harbor ont très fortement mobilisé la CNIL. La Présidente de la CNIL a été réélue à la présidence du G29 (groupe des CNIL européennes) en février 2016, pour un mandat de deux ans.

Réagissez à cet article