Que sait de nous Google grâce à nos comportements sur Internet ?

	Que sait de nous Google grâce à nos comportements sur Internet ?

Mondialement connue, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps…). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits…

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Moutain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook…) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa…

Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

… en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée…

L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous** ! »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*

Que fait Auchan avec notre ticket de caisse ?

Que fait Auchan avec notre ticket de caisse ?

Anticipation de pénurie, état des stocks, performance des zones commerciales… rien n'échappe aux caisses connectées du groupe nordiste.

Nos tickets de caisse sont des mines d'informations! Si on imagine d'emblée qu'une connaissance précise de notre consommation individuelle, destinée à proposer des offres ciblées, constitue un graal pour les Carrefour, Leclerc et consorts, ce n'est pas forcément l'intérêt premier qu'y voient les professionnels de la grande distribution.

Ainsi, pour le groupe Auchan, c'est d'abord à un juste réapprovisionnement des rayons que servent les informations enregistrées par les 7.000 caisses connectées de ses hypermarchés. Remontées en temps réel vers la base de données installée par l'Américain Teradata en région lyonnaise, les données de nos facturettes nourrissent ensuite une appli développée en interne par les services informatiques du groupe détenu par la famille Mulliez. Dès lors, les salariés peuvent connaître en temps réel l'état de leur rayon par produit, au sein de chaque magasin. Ainsi, le responsable du rayon boissons non-alcoolisées peut, grâce à une icône, savoir si son rayon manque partiellement d'une référence ou, selon le jargon maison, s'il est « fantôme », c'est-à-dire vide.

« Pour certains rayons, tels que les sandwiches entre 12h et 14h, c'est anticipable. L'intérêt est donc pour nous de détecter d'autres comportements du consommateur qu'on ne peut prévoir… Un rayon peut être dévalisé en un rien de temps par une personne ou un groupe de personnes, de façon imprévisible ou bien en fonction d'une promotion. En ce sens, l'application peut fournir une information utile au chef de gondole », estime Eric Dewilde, directeur architecture et données au sein du groupe Auchan. Parce que rien ne vaut l'œil humain, les salariés utilisateurs de l'appli sont amenés à faire un retour d'expérience pour dire si le réassort est en cours ou s'il s'agit d'une fausse alerte. *« Nous sommes en phase de rodage. En outre, on n'envoie pas de « push » pour signifier que le rayon se vide. Le principe est de délivrer une information, pas un ordre »,* précise-t-on au sein d'Auchan…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Ce qu'Auchan fait vraiment de nos tickets de caisse – Challenges.fr*

Big data. Comment les entreprises recueillent et utilisent nos données ?

	Big data. Comment les entreprises recueillent et utilisent nos données ?

En 2015, 11 % des entreprises françaises ont traité des big data, selon l'Insee. Les sources de données les plus utilisées sont la géolocalisation, les médias sociaux et les objets connectés ou capteurs. Les grosses entreprises sont les plus à l'aise pour traiter ces données nombreuses et complexes.

Par Julie DURAND

1 % des entreprises françaises ont traité des big data en 2015. Selon l'Insee, qui a réalisé cette enquête, la big data est constituée de » **données complexes, dont le volume important et l'actualisation constante rendent difficile l'exploitation par les outils classiques** « .

7 % des entreprises traitent des données de géolocalisation

Sans surprise, les grosses entreprises sont plus nombreuses à en utiliser que les petites (24 % contre 9 %). Les barrières à l'utilisation de la data sont plus difficiles à franchir pour elles : mauvaise compréhension du sujet et de son intérêt, manque de compétences, coût trop élevé et législation contraignante.

La donnée la plus recueillie et la plus utilisée est la géolocalisation (pour 62 % des entreprises qui utilisent des data, soit 7 % de l'ensemble des entreprises françaises). Cette donnée intéresse surtout les entreprises de transports (92 %) et la construction (89 %).
Deuxième source : les médias sociaux (pour 32 % des entreprises qui utilisent des data, soit 4 % de l'ensemble). Ces données intéressent surtout l'hébergement-restauration (76 %) et l'information-communication (64 %).
Enfin, les objets connectés et capteurs sont la troisième source de data (29 % des entreprises qui en utilisent, soit 3 % de l'ensemble), utilisés principalement par l'industrie (46 %).

Traitement en interne ou externalisée des données ?

74 % des entreprises qui traitent des données le font en interne et 42 % par des prestataires extérieurs, 16 % utilisent donc ces deux méthodes. Le choix entre traitement interne ou externe dépend du secteur et de la taille de l'entreprise. 90 % des entreprises de l'infomation-communication et 84 % des activités scientifiques et techniques le font en interne, » **car les employés sont probablement mieux formés pour cela que dans d'autres secteurs** ». Tous secteurs confondus, 83 % des entreprises de plus de 250 personnes traitent les data en interne, contre 73 % pour les moins de 250 salariés.
Selon l'Insee, les entreprises utilisent toutes ces données pour optimiser leurs processus internes, améliorer leurs produits ou services et/ou rendre plus efficace leur marketing ou leur gestion des ventes.

Réagissez à cet article

Source : *Big data. Comment les entreprises recueillent et utilisent nos données ?*

Le Règlement Général sur la Protection des Données (RGPD) en détail

Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants.
Intitulé *« Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »*, le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que *« 96% des entreprises des trois principales économies européennes [France, Allemagne, Royaume-Uni] ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) (…) Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD »* !
Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitant des données personnelles de citoyens européens sont concernées par le Règlement.
Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD
Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises.
Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative.
Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc …). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :
• Restriction d'utilisation ;
• Minimisation des données ;
• Précision ;
• Limitation du stockage ;
• Intégrité ;
• Confidentialité.
Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La *« pseudonymisation »* consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données
Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : *« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »* (Article 35 du Règlement)
Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement : les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (*« privacy by design and by default »*).

2. Consentement clair et explicite à la collecte des données
La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposé de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*.
Ce consentement doit donc être express. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu' *« il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité. »* Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°).
Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f)) :
• Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
• Lorsque le traitement découle d'une obligation légale ;
• Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
• Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
• Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données
Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : *« la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais »* (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)
A l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas *« d'accès non autorisé »* à des données personnelles. En clair, lors d'un piratage. Le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, en ce compris leurs sous-traitants, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlementindique que ce signalement devra intervenir *« lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. »* L'emploi du mot *« élevé »* laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante.
Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire
Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle.
Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de la démontrer.
Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou *« data processor »*, même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuit.

6. Création des délégués à la protection des données (Data Protection Officer)
Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le *« CIL »*), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPD ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont *« les activités de base (…) exigent un suivi régulier et systématique à grande échelle des personnes concernées »* ou lorsque *« le traitement est effectué par une autorité publique ou un organisme public »* (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre comptes à l'autorité de contrôle de l'état de ses traitements de données.
Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même
Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données.
En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présentent l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement.
Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou *« droit à la portabilité des données »*) vers un autre fournisseur de services : *« Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle »* (Article 20).

8. Restriction du profilage automatisé servant de base à une décision
L'article 21 du Règlement dispose que *« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »*, sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions
La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice.
Le Règlement prévoit quant à lui un *« droit à un recours effectif »* (articles 78 et 79) et un *« droit à réparation »* (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux…[lire la suite]

Notre métier :
Nous proposons des service d'accompagnement sur plusieurs niveaux :
1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.
1'/ Au niveau des utilisateurs encore pour sensibiliser les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes.
Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FOVI et à voir leurs procédures auditées et probablement améliorées.
2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.
3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses misions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.

Les données de santé, la nouvelle cible des cybercriminels

Les données de santé, la nouvelle cible des cybercriminels

Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

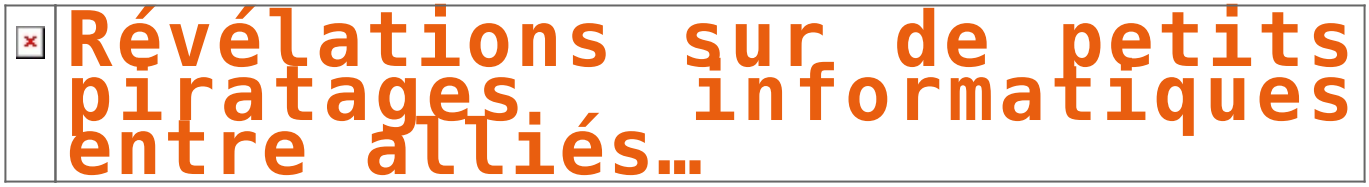
Une centralisation des données qui n'est pas sans risque

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.
Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.
Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.
Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 $.
Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.
Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.
Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Les données de santé, le nouvel El-Dorado de la cybercriminalité

Révélations sur de petits piratages informatiques entre alliés…



C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.
Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »
Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »
Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Géolocaliser un téléphone mobile en deux clics de souris

Cyber géolocaliser un porteur de téléphone est de plus en plus simple. Un chercheur en informatique montre à ZATAZ.COM comment créer un tracker maison devient simple comme bonjour.

Les téléphones portables, de nos jours, sont de véritables ordinateurs aux capacités de traçage, surveillance et cyber surveillance qui fait froid dans le dos. Regardez, prenons les exemples tels que Facebook et son option « amis à proximité » ou encore PokemonGo et sa capacité de géolocalisation. Du traçage au centimètre. Des technologies de « ciblage » qui deviennent simple à créer et à utiliser. Tristan, informaticien Parisien, vient de contacter ZATAZ pour présenter son cas d'étude : un outil de traçage en temps réel capable de tracer l'itinéraire de ses cibles.

Géolocaliser un téléphone : **Souriez, vous êtes pistés**
Depuis quelques temps Tristan s'intéresse aux applications proposées dans les mobiles, et plus précisément aux logiciels qui font transiter des informations telles que des positions de latitude et de longitude. Avec un associé, il a lancé Lynx Framework, une entité spécialisée dans la création d'outils de sécurité pour les applications web.
A parti de ses recherches, Tristan a créé un outil de « traque », de quoi géolocaliser un téléphone qui met à jour les dangers de nos mobiles et de leurs capacités à indiquer notre emplacement, mais aussi, nos itinéraires. « ***En analysant les requêtes envoyées par certaines applications je me suis rendu compte qu'il serait possible de récupérer le positionnement de plusieurs personnes en même temps et de les positionner sur une carte de type google map.*** » m'explique le chercheur.

A l'image des sauvegardes de Google Map que je vous indiquais en 2015, l'outil « privé » de Tristan fait pareil, mais en plus discret encore. Via un outil légal et disponible sur Internet, Burp Suite, notre chercheur a analysé les requêtes envoyées par plusieurs logiciels de rencontres disponible dans le Google Play.

Comment cela fonctionne-t-il ?
« *Le tracker prend le contrôle de plusieurs comptes d'application de rencontre et récupère la position des personnes à proximité,* indique-t-il à ZATAZ.COM. *Il ajoute ces informations dans sa base de données et vérifie l'existence des positions pour cette identité. » Si l'application de Tristan retrouve la même personne, mais pas à la même position, il va créer un itinéraire de l'individu via son ancienne position*« . Nous voilà avec la position et le déplacement exacts d'un téléphone, et donc de son propriétaire, à une heure et date données.

Géolocaliser un téléphone : Chérie, tu faisais quoi le 21 juillet, à 12h39, à 1 cm de ta secrétaire ?
Après quelques jours de recherche, Tristan a mis en place une base de données de déplacement dans une ville. Une commune choisie au hasard. Son outil est en place, plusieurs systèmes sont lancés : Une carte avec le positionnement des personnes croisées ; une page plus explicite pour chaque personne avec la date de croisement, son âge… ; une page ou notre chercheur gère ses comptes dans l'application. Bonus de son idée, un système d'itinéraire complet a été créé. Il permet de tracer un « chemin » de déplacement si la personne croisée a déjà été croisée dans le passé, dans un autre lieu. « J'ai positionné un compte au centre de la ville, un autre à l'entrée et le suivant à la sortie, ce qui a données en quelques heures une 50ène de données » confie-t-il « Il est inquiétant de voir autant de données personnelles transitées en clair via ces applications ».

Géolocaliser un téléphone : détournement possible d'un tel « tracker » ?
Vous l'aurez compris, « tracer » son prochain est facilité par ses applications qui ne protègent pas les informations de positionnement des utilisateurs. Il devient possible d'imaginer une plateforme, en local, avec plusieurs comptes positionnés à des endroits différents dans une ville. Bilan, suivre plusieurs individus devient un jeu d'enfant. Si on ajoute à cela les applications de déplacement de type UB, qui communique les données de ses chauffeurs par exemple, ainsi que celles d'autres réseaux sociaux, il devient réellement inquiétant de se dire que positionner une personne et la tracer se fait en quelques secondes. Deux solutions face à ce genre de traçage : jeter votre portable ou, le mieux je pense, forcer les éditeurs d'applications à vérifier la sécurisation des données envoyées, et les chiffrer pour éviter qu'elles finissent en clair et utilisable par tout le monde.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Géolocaliser un téléphone mobile en deux clics de souris – ZATAZ

Quelques domaines d'application du Big Data dans les Comment les données améliorent les services

communaux | L’Atelier : Accelerating Innovation

Quelques domaines d’application du Big Data

Conscients du potentiel que représentent le recueil et l'analyse de données pour leur fonctionnement, les gouvernements leur accordent une attention croissante. Tour d'horizon des domaines d'application du Big Data.

« *Les données sont le nouveau pétrole : les villes, notamment, prennent conscience de leur valeur et du bénéfice qu'elles peuvent en tirer pour améliorer l'usage de leurs infrastructures et la qualité des services dispensés à leurs citoyens.* ». C'est ce qu'a déclaré récemment Arvind Satyam, chargé du développement des affaires internationales pour le projet Internet of Everything de CISCO Systems. Cependant, « *si la plupart des villes ont conscience de leur valeur, beaucoup ignorent comment les valoriser.* » Une étude sur le numérique aux Etats-Unis réalisée par le cabinet McKinsey classe le gouvernement à la 18e place, sur un total de 22 acteurs, en ce qui concerne l'adoption des technologies numériques. Un retard technologique qui se traduit directement en monnaie sonnante et trébuchante. Toujours selon cette étude, l'usage du *Big Data* par les autorités publiques permettrait d'épargner 460 milliards de dollars d'ici 2020.

Et plus qu'un enjeu économique, comme le note dans un billet de blog, Shaina Doar, du Sidewalk Labs, filière de Google aidant les communes à passer à l'ère de la smart city, ce chiffre « *représente une immense opportunité ratée de révolutionner l'accès à la santé, l'éducation, la sécurité et autres services de base, et par conséquent, d'améliorer grandement la qualité de vie des Américains.*» Les choses sont pourtant en train d'évoluer. Un nombre croissant d'états américains se dotent de data scientists et plusieurs rapports mettent en exergue le potentiel d'une utilisation avisée des données, pour une meilleure qualité des services publics.

Améliorer la mobilité…

De manière très concrète, les autorités peuvent se targuer, grâce au *Big Data* d'améliorer la qualité des services fournis aux citoyens. Le potentiel pour une meilleure gestion des flux de mobilité urbaine est particulièrement évident. Un bon usage des données aide par exemple à repérer les places de parking disponibles, à les communiquer aux automobilistes pour favoriser un stationnement plus rapide et réduire ainsi le trafic. Des feux tricolores intelligents, servis par les données, offrent dans certains territoires une meilleure régulation de la circulation. La conception d'applications de navigation holiste rassemblant l'ensemble des données issues des différents moyens de transport disponibles, du vélo à la voiture individuelle en passant par le tramway et l'autopartage, optimise les déplacements des individus. La start-up Placemeter propose de son côté de communiquer l'ensemble des données, ayant trait aux flux de population urbaine aux municipalités, pour permettre à ces dernières d'optimiser la gestion de l'espace public. « *Nous pouvons désormais savoir où les individus passent le temps dans la ville, et à quel moment. Ainsi, si telle place publique connaît un pic d'affluence chaque jour entre 17 et 19h, la municipalité peut adapter ses services, renforcer la sécurité ou réaménager l'espace public pour prendre en compte cette réalité.* » explique Arvind Satyam. Cisco et Placemeter travaillent ainsi en collaboration avec la Mairie de Paris pour analyser les flux de population sur la Place de la Nation, dans le cadre du projet de rénovation de cette place, porté par la Mairie.

A Chicago, le Big Data *permet de détecter les infractions sanitaires dans les restaurants.*

…et les services publics

Outre l'amélioration de la mobilité, l'usage du *Big Data* permet aux gouvernements d'optimiser leurs services dans de nombreux domaines. Prenons la salubrité publique, par exemple. A Chicago, le Department of Innovation and Technology a récemment mis au point un algorithme permettant de prédire les infractions au code sanitaire dans les restaurants. Prenant en compte neuf variables, dont l'historique des infractions commises par les restaurants, la durée depuis la dernière inspection ou encore la dangerosité et la propreté de la zone géographique, l'algorithme détecte les infractions graves, en moyenne sept jours plus tôt que le système traditionnel. La ville de Chicago comptant trois millions d'habitants et 15 000 restaurants pour seulement une trentaine d'inspecteurs sanitaires, une allocation optimale des ressources est capitale pour garantir une meilleure protection des citoyens. Les mégadonnées peuvent également venir en aide aux plus démunis : ainsi, à New-York, l'entreprise SumAll a recours à l'analyse de données pour repérer les ménages risquant d'être évincés de leur logement et les aider à s'en sortir.

New-York a recours aux données pour aider les plus démunis.

Vers des services personnalisés

Le *Big Data* permet également aux pouvoirs publics de personnaliser leurs services, fournissant des prestations adaptées à chaque situation individuelle plutôt que des offres standards taillées pour un profil-type inexistant. Ainsi, plusieurs villes américaines ont adopté un outil baptisé the Public Safety Assessment, qui utilise les mégadonnées pour aider les juges à déterminer si un suspect doit être détenu avant son procès ou s'il peut être laissé en liberté. L'outil repose sur des données recueillies parmi un million et demi de cas différents recueillis auprès de 300 juridictions américaines. Il prend en compte les antécédents judiciaires de l'accusé, les faits lui étant reprochés et son âge. The Public Safety Assessment permet ainsi de réduire à la fois le taux d'incarcération et le nombre de crimes commis par des individus en attente d'un procès. Dans un autre registre, à Singapour, l'application Beeline offre aux citoyens de remonter leurs requêtes, pour des routes plus adaptées à leurs besoins.

Renforcer la confiance dans le gouvernement

Le *Big Data* est aussi un outil efficace pour renforcer la confiance des citoyens dans le gouvernement, en oeuvrant pour la transparence. « *Je pense que l'ouverture des données peut contribuer à plus de transparence, à éclairer les citoyens sur les actions du gouvernement, afin qu'ils sachent où vont leurs impôts, qu'ils voient l'intérêt de participer au processus démocratique.* » confiait Libby Schaaf, maire d'Oakland, à L'Atelier l'an passé. Dans cette optique, la ville d'Oakland s'est doté d'un site internet baptisé Open budget Oakland. Il offre une visualisation exhaustive et intelligible du budget de la ville, afin que les citoyens puissent savoir où vont leurs impôts. Cette infographie a été conçue par les jeunes bénévoles d'Open Oakland qui mettent les nouvelles technologies au service de la collectivité, et travaillent notamment sur l'ouverture et l'exploitation des données. La mairie de la ville met de son côté des locaux à leur disposition. Lors de la dernière élection municipale, les jeunes volontaires ont également conçu une infographie mettant en évidence les sources de financement des différents candidats. De quoi rendre le processus électoral moins opaque et plus digne de confiance.

« *Les gouvernements peuvent accroître leur capital confiance en donnant aux citoyens accès aux données, et en leur offrant ainsi une meilleure visibilité sur le monde qui les entoure.* », affirme Arvind Satyam. Car telle la matière noire bien connue des scientifiques, les données sont invisibles mais agissent sur notre environnement.

Oakland compte parmi les villes pionnières en matière d'Open Data.

Donner plus de pouvoir aux citoyens

Promouvoir l'usage des données sert aussi à renforcer les échanges entre citoyens et gouvernements, participant à l'établissement de ce lien de confiance qui fait aujourd'hui souvent défaut. La start-up NextRequest propose ainsi une plate-forme intuitive permettant de demander l'accès à n'importe quel document public. Mis en place par la municipalité d'Asheville, le site SimpliCity communique de son côté n'importe quelles données concernant la ville, qu'il s'agisse des chiffres de la criminalité, du montant des taxes ou encore des projets immobiliers. L'application NYC311 autorise les New-Yorkais à alerter les autorités en cas de problème concernant un bien ou service public, qu'il s'agisse d'une absence de collection des déchets, d'un parcmètre défectueux ou encore d'une école vandalisée. Lors de l'hiver 2015, qui fut particulièrement rigoureux dans l'est des Etats-Unis, plusieurs villes, dont Boston et Chicago, se sont dotées d'applications permettant aux citoyens de signaler les tronçons de route enneigés ou verglacés. Chaque fois, la même volonté de rapprocher le citoyen des pouvoirs publics et de rendre la démocratie plus transparente et efficace.

A Montréal, l'application Ubifood permet de lutter contre le gaspillage alimentaire.

Renforcer les liens communautaires

Enfin, le Big Data est un moyen de renforcer l'engagement civique des individus, de souder la communauté et d'améliorer son fonctionnement. A Jakarta, où la collecte des déchets pose un véritable défi aux pouvoirs publics, grâce à une application, les citoyens indiquent les zones géographiques où collecter les déchets. Et les habitants peuvent s'improviser éboueurs en échange d'une somme d'argent. A Montréal, l'application Ubifood rend possible pour les magasins ayant des stocks de nourriture proche de la date de péremption de publier des offres promotionnelles sur ces produits. Les utilisateurs de l'app voient alors d'un clic les offres situées dans leur zone géographique, paient via l'application et passent récupérer leurs achats au magasin. Citons finalement l'application MyResponder, développée à Singapour, qui avertit les citoyens disposant d'une formation en secourisme lorsqu'une personne fait un malaise dans la rue à proximité. Aussi abstraites qu'elles puissent paraître, les données peuvent ainsi sauver des vies.

Article original de Guillaume Renouard

Réagissez à cet article

Original de l'article mis en page : Comment les données améliorent les services communaux | L'Atelier : Accelerating Innovation

---

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

Microsoft stocke 200 Mo de données informatiques sous forme d'ADN

L’université de Washington a collaboré avec Microsoft pour écrire 200 Mo de données informatiques sur un bout d’ADN. Le but est d’optimiser au maximum l’espace de stockage et sa durabilité en allant vers un stockage biologique.

Écrire 200 méga-octets de données informatiques sur de l’ADN de synthèse. C’est la prouesse réalisée par des scientifiques de l’université de Washington en collaboration avec Microsoft. Les informations inscrites sur les molécules contiennent la Déclaration universelle des droits de l’homme en plus de 100 langues, les 100 livres électroniques les plus téléchargés sur la bibliothèque Projet Gutenberg, une partie des bases de données de Crop Trust, un groupe consultatif international pour la recherche agricole et un clip musical du groupe américain Ok Go,
« *Nous utilisons l’ADN comme un espace de stockage de données numériques* », explique le professeur Luis Ceze dans une vidéo. « *La raison pour laquelle nous faisons cela est parce que l’ADN est très dense et que l’on peut mettre énormément d’informations dans un très petit volume* », ajoute-t-il.

LA TOTALITÉ DE L’INTERNET POURRAIT TENIR DANS UNE BOÎTE À CHAUSSURES
Il affirme également que la totalité de l’Internet pourrait tenir dans une boîte à chaussures grâce à ce procédé. L’autre motivation des scientifiques est aussi le fait que l’ADN peut être conservé très longtemps. « *Dans les bonnes conditions, il peut durer des milliers d’années tandis que les technologies de stockages ne tiennent que quelques décennies* ».

L’ADN est fait de différentes séquences de quatre molécules : l’adénine (A), la guanine (G), la cytosine (C) et la thymine (T).Les scientifiques ont réussi à encoder les données qu’ils voulaient stocker sur les quatre molécules de base de l’ADN synthétisé.
En analysant l’ADN, ils peuvent lire les informations et les rétablir à leur état original.
Les 200 Mo de documents sont enregistrés sur un bout d’ADN qui fait la taille de quelques grains de sucre. Celui-ci a été encapsulé pour éviter toute dégradation.
Les capacités de stockage de l’ADN sont énormes. Malheureusement, lire les données dessus prend beaucoup de temps – jusqu’à plusieurs heures. Aussi, ce procédé n’est pas prêt d’être démocratisé, d’autant plus qu’il coûte encore très cher. Mais cela serait apparemment en train de changer. « *La technologie pour lire l’ADN est en train de se développer rapidement et pourrait devenir suffisamment rapide et bon marché pour être commercialisée* », explique Luis Ceze à The Register.
Le scientifique pense que les premiers clients seront probablement les centres de données pour qui l’optimisation de l’espace de stockage est un enjeu permanent.

Article original de Omar Belkaab

Réagissez à cet article

Original de l’article mis en page : Microsoft stocke 200 Mo de données informatiques sous forme d’ADN – Sciences – 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

Réagissez à cet article

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