Les États-Unis font voler en éclat les règles protégeant la vie privée sur Internet

Les États-Unis font voler en éclat les règles protégeant la vie privée sur Internet

De la mobilisation des lobbys à la signature du président, The Washington Post démonte le processus qui a conduit à la suppression d'une réglementation adoptée sous l'ère Obama, qui encadrait la vente de données personnelles par les fournisseurs d'accès à Internet.

Fin mars, les Américains ont eu la mauvaise surprise de voir leur Congrès voter l'abolition de nouvelles règles destinées à protéger leur vie privée sur Internet. Adoptées sous l'administration Obama, ces règles empêchaient les fournisseurs d'accès américains tels que Comcast ou AT & T de stocker et de vendre les données de leurs clients, issues de leur historique de navigation, sans leur consentement. Elles n'auront pas eu le temps d'entrer en vigueur…[lire la suite]

Réagissez à cet article

Source : *États-Unis. Comment les républicains ont démantelé des règles protégeant la vie privée sur Internet | Courrier international*

Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l’Intelligence Artificielle

	Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l’Intelligence Artificielle

Prévenir plutôt que guérir : si la grande majorité des médecines traditionnelles de par le monde appliquent déjà ce principe depuis des milliers d'années, il semblerait que la technologie puisse intégrer, elle aussi, ce principe de prévention. Et c'est bien l'intention de Google avec ce nouveau développement de son pôle de recherche scientifique, Google Brain. Cela donnerait un coup de pouce géant à certains domaines de la médecine moderne, notamment en termes de prévision et prévention des maladies cardio-vasculaires, de plus en plus nombreuses, chez les hommes comme chez les femmes.
Google s'est associé avec les universités américaines de Chicago et de San Francisco, afin de concevoir une technologie qui, grâce à l'intelligence artificielle et aux données récupérées par les hôpitaux parmi les milliers de dossiers médicaux des patients, permettrait de pouvoir prédire des risques médicaux, une projection de l'état de santé post-hospitalisation, ou les arrêts cardiaques, entre autres espérances…[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 : *Intelligence artificielle : Google veut jouer à Madame Irma et anticiper les problèmes de santé*

Google tente d'arrêter une attaque de phishing sur Gmail

Google tente d'arrêter une attaque de phishing sur Gmail

Cette tentative de hameçonnage a tenté de faire croire aux utilisateurs ciblés qu'ils étaient en liaison avec Google Docs. Moins de 0,1% des utilisateurs de Gmail ont été touchés, assure Google.
Le courrier électronique provenait de l'adresse réelle d'un contact connu et demandait de cliquer sur un lien censé conduire à un fichier partagé avec le service en ligne de Google Docs. En cliquant sur le lien, on arrivait sur une véritable adresse web de Google et une autorisation pour exécuter une application que le(s) hackers(s) avait(ent) habilement appelée « Google Docs » était demandée…[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 : *Cybersécurité : Google essuie une attaque de phishing sur Gmail – Les Echos*

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*

Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017

Secret des correspondances : Ce que change la loi Lemaire à partir de 2017

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

La correspondance privée se définie comme tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courriel échangé entre deux ou plusieurs correspondants, depuis un service de messagerie.

Ainsi, toute correspondance entre deux personnes doit être protégée au titre du secret, par les opérateurs dont l'activité consiste à acheminer, transmettre ou transférer le contenu de ces correspondances. Tout comme un facteur n'a pas le droit d'ouvrir un courrier postal, le fournisseur de messagerie électronique ou le fournisseur d'accès à internet sont tenus de respecter le secret des courriers électroniques.

Ce principe de confidentialité était d'ailleurs déjà garanti par l'article L32-3 du Code des postes et des communications électroniques qui prévoyait, dans sa version antérieure à la publication de la loi pour une République numérique que « *les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances* ».

La directive européenne 2002/58 modifiée relative à la vie privée dans les communications électroniques (l'article 5.1) interdit « *à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs* ».

Le contenu des communications, c'est-à-dire des correspondances entre deux individus, est par principe confidentiel et l'obligation de garantir le secret repose sur les opérateurs de télécommunication.

Il est en revanche possible de lever le secret des correspondances, en demandant aux personnes concernées leur consentement.

Qu'est-ce qui change avec la loi pour une République numérique et son décret d'application relatif à la confidentialité des correspondances ?

L'article 68 de loi pour une République numérique précise ce que couvre le secret des correspondances. Ce secret s'applique ainsi à l'identité des correspondants, au contenu, à l'intitulé et aux pièces jointes des correspondances.

Quels sont les professionnels concernés ?

Sont désormais soumis au respect du secret des correspondances, à la fois les « *opérateurs* », c'est-à-dire les opérateurs de télécommunications essentiellement, et les « *fournisseurs de services de communication au public en ligne* », en d'autres termes, tout acteur permettant à deux personnes de correspondre en ligne. Seront notamment concernés les fournisseurs de services de messagerie électronique, de réseaux sociaux, de communication synchrone (VoIP), etc.

A quelles conditions peuvent-ils exploiter la correspondance privée ?

La loi Lemaire leur permet toutefois d'exploiter la correspondance privée, **sous réserve d'obtenir le consentement des utilisateurs et pour les seules finalités suivantes** :

- l'amélioration du service de communication au public en ligne,
- la réalisation de statistiques,
- l'utilisation des données à des fins publicitaires.

Quels sont les effets en pratique pour les opérateurs de communication électronique ou fournisseurs de service ?

La CNIL rappelle que, pour être valable, ce consentement doit être libre, spécifique et informé. Il doit en outre résulter d'un acte positif et être préalable à la collecte des données, c'est-à-dire à la réalisation du traitement.

Un consentement informé

Les opérateurs souhaitant utiliser la correspondance de leurs utilisateurs à des fins statistiques, publicitaires ou encore pour améliorer leur service devront recueillir leur consentement spécifique après les avoir informés de ce qu'ils souhaitent faire (en rappelant les mentions requises par l'article 32 de la loi Informatique et libertés).

Un consentement spécifique

La CNIL rappelle que le consentement doit être spécifique et qu'à ce titre, un consentement global pour plusieurs finalités différentes, de même que l'acceptation globale des Conditions générales d'utilisation (ou CGU) du service, **ne peuvent être considérés comme un consentement valable**.

Un consentement libre

Le consentement ne doit pas être contraint, c'est-à-dire que le refus de consentir ne doit pas empêcher la personne d'accéder au service de messagerie. Le consentement doit prendre la forme d'un acte positif des utilisateurs et ne peut donc être déduit du silence ou de l'inaction des utilisateurs. Le consentement devant être recueilli avec une périodicité d'un an, la CNIL recommande que les responsables de traitement alerte les personnes dans un délai raisonnable avant l'échéance de ce délai, pour que le renouvellement ne soit pas automatique.

Un consentement renouvelé tous les ans

La loi pour une République numérique prévoit que le consentement doit être renouvelé périodiquement, c'est-à-dire recueilli tous les ans par les opérateurs exploitant les correspondances.

Par ailleurs, la CNIL rappelle que les traitements réalisés sur les correspondances doivent se limiter aux données collectées de manière loyale et licite. En conséquence, les traitements ne doivent produire des effets qu'à l'égard des personnes qui ont valablement consenti à la collecte de leurs données à caractère personnel issues du contenu de leurs correspondances. À titre d'exemple, les traitements opérés à des fins publicitaires et basés sur le contenu des correspondances ne doivent pas permettre à l'opérateur de cibler d'éventuelles personnes tierces dont les données personnelles apparaitraient dans la correspondance.

Enfin, la CNIL rappelle qu'une fois le règlement européen relatif à la protection des données, adopté, les responsables de traitement devront être en mesure de prouver que les personnes ont effectivement consenti au traitement et seront tenus de les informer de la possibilité de retirer leur consentement.

Réagissez à cet article

Source : *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique | CNIL*

Alerte : Faille de sécurité dans le gestionnaire de mots de passe LastPass

Alerte : Faille de sécurité dans le gestionnaire de mots de passe LastPass

---

LastPass fait partie des gestionnaires de mots de passe les plus populaires. Néanmoins, sa sécurité semble laisser à désirer. Une nouvelle fois, une faille a été dénichée pouvant permettre – en théorie – de voler les identifiants et les mots de passe des utilisateurs.

Ici, la faille a été remarquée au niveau de l'extension Firefox de LastPass. Le chercheur en sécurité Tavis Ormandy, qui travaille chez Google, a dévoilé certaines informations et note qu'une personne mal intentionnée aurait pu se faire passer par un serveur de LastPass pour émettre des messages à l'utilisateur. Or, les messages n'auraient pas été authentifiés et l'auteur aurait pu être en mesure d'avoir des accès avec privilèges élevés, ce qui lui aurait permis de faire une copie des identifiants et mots de passe enregistrés.
Fort heureusement, LastPass a été mis au courant et a surtout corrigé la faille. Une mise à jour de l'extension Firefox est actuellement disponible, elle sera automatiquement téléchargée chez les utilisateurs. Il est possible de forcer la mise à jour en se rendant dans la section des modules complémentaires de Firefox, de faire une recherche manuelle et de lancer l'installation dans la foulée…[lire la suite]

Réagissez à cet article

Source : *Le gestionnaire LastPass bouche une faille qui permettait de récupérer les identifiants des utilisateurs | KultureGeek*

« iPhone à 1 € !!!! » : l'Europe épingle Facebook,

Twitter et Google sur les publicités mensongères

	« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères

Publicités, confidentialité ou encore respect des droits des consommateurs : Bruxelles a souhaité mettre au clair ses demandes auprès des grands réseaux sociaux. Épinglés par l'Union sur différent dossiers, Facebook, Google et Twitter ont désormais un mois pour appliquer les changements exigés.

Ce vendredi, la Commission européenne a finalement mis en demeure les trois principaux réseaux sociaux (Facebook, Twitter et Google+) qui agacent Bruxelles sur de nombreux dossiers.
Avertie notamment par les régulateurs de concurrence des pays de l'UE, la Commission voulait mettre fin à de nombreuses pratiques publicitaires illégales au sein des frontières européennes. Mais Bruxelles ne s'en est pas tenu à une simple auscultation des publicités des réseaux, l'exécutif européen a également tenu à évaluer minutieusement la gestion des données personnelles et la réactivité des réseaux face aux contenus illégaux.

UN MOIS POUR EN FINIR AVEC LES IPHONE À 1€

Désormais, après avoir rencontré ce jeudi les autorités européennes, les entreprises, Facebook, Twitter et Google, disposent d'un mois pour changer leurs pratiques en adéquations avec les exigences légales. Les autorités auraient proposé aux dirigeants certains aménagements pour s'adapter au cadre juridique européen selon Reuters.
Dans le viseur de la Commission, les procédures juridiques entre consommateur européen et société américaine. Pour Věra Jourová, commissaire européenne chargée de la justice, « *il est inacceptable que les consommateurs de l'Union puissent seulement saisir une juridiction californienne en cas de litige.* »

Mais elle n'a pas épargné la publicité mensongère, les arnaques, et le contenu sponsorisé mal identifié : la Commission a notamment visé les fameuses arnaques qui proposent « ***des iPhone ou iPad à 1 euro mais étant associées à un abonnement de longue durée caché, pour plusieurs centaines d'euros par an*** » explique les autorités bruxelloises qui prennent très au sérieux cette affaire.
Du côté des grandes entreprises américaines, Google assure déjà procéder à un examen approfondi de ces conditions. Facebook et Twitter préfèrent encore garder le silence sur les requêtes de Bruxelles.
En dehors des dossiers publicitaires, qui sont nécessairement sensibles pour les deux sociétés, la question de la modération et de la gestion de contenus calomnieux reste un problème douloureux du côté de Facebook comme du côté de Twitter. Les deux réseaux sont par ailleurs également pressés par l'Allemagne qui exigera prochainement une réactivité forte dans la lutte contre la désinformation et la calomnie sur les plateformes, sous peine sinon de voir la République Fédérale pénaliser Facebook d'une amende pouvant aller jusqu'à 50 millions d'euros.

Réagissez à cet article

Source : *« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères – Politique – Numerama*

Google, ou la révolution transhumaniste via le Big Data

Google, ou la révolution transhumaniste via le Big Data

A l'occasion de la sortie du livre de Christine Kerdellant Dans la Google du loup, Éric Delbecque décrypte le projet de « fusion » entre le vivant et le digital porté par le géant de l'informatique américain.

Christine Kerdellant a relevé un beau défi *Dans la Google du loup* (Plon)! Elle met le doigt là où Google pose véritablement problème, à savoir sur la révolution anthropologique du transhumanisme… Pour ce qui concerne sa participation à la société de surveillance globale que fabriquent un certain nombre d'acteurs publics et privés, l'affaire est entendue depuis des années… Sous l'administration Obama, les dirigeants de Google se rendirent à la Maison-Blanche 230 fois! Ils confirmèrent en 2013 que les agences gouvernementales de l'Oncle Sam les sollicitaient annuellement – dans le cadre du Patriot Act – pour surveiller 1000 à 2000 comptes. En janvier 2015, la firme vedette du Web a reconnu avoir fourni au Ministère de la Justice américain l'intégralité des comptes Google de trois membres de WikiLeaks.
Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons.
Il paraît dès lors compliqué de penser qu'une idéologie sécuritaire explique à elle seule l'extension de l'ombre de Big Brother sur le monde. Les géants du numérique du secteur privé (les GAFA: Google, Amazon, Facebook, Apple) participent largement à la manœuvre, plus ou moins volontairement (pas pour des raisons politiques, mais économiques). Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons. Sa stratégie en matière de renseignement doit se lire comme un fragment d'un système cybernétique (au sens de science du contrôle) beaucoup plus vaste, où le capitalisme financier californien et numérique occupe une place décisive. Séparer ce dernier du complexe militaro-sécuritaro-industriel de l'Oncle Sam devient de plus en plus difficile, voire hasardeux.
L'intérêt plus décisif du livre de Christine Kerdellant est ailleurs. Il explore de manière très accessible et percutante le cœur du projet Google, ou plutôt sa signification philosophique profonde. Derrière les joyeux Geeks de la Silicon Valley s'exprime la volonté de réifier l'humanité, de l'enchaîner à une raison calculante. Cette dernière va nous émanciper nous répète-t-on, nous libérer – via le Big Data – des limites de notre condition, nous délivrer de la mort et transformer notre existence en un jardin de fleurs. Mais lorsqu'on choisit d'examiner de plus près les conséquences des propositions de Google, on découvre une perspective d'avenir moins réjouissante…[lire la suite]

Réagissez à cet article

Source : *Google, ou la révolution transhumaniste via le Big*

Data

Les messages de WhatsApp peuvent être facilement lus par la CIA

	Les messages de WhatsApp peuvent être facilement lus par la CIA

L’organisation WikiLeaks a reçu une importante base de données révélant les techniques de cyber-surveillance et de piratage de la CIA. Selon ces informations l’agence de renseignement américaine peut facilement accéder aux messageries, y compris WhatsApp et Telegram.

La Central Intelligence Agency (agence centrale de renseignement, CIA) est capable de contourner le cryptage de certaines applications populaires de messagerie, y compris WhatsApp et Telegram, selon les documents publiés par WikiLeaks aujourd’hui.
« Ces techniques permettent à la CIA de contourner le cryptage de WhatsApp, de Signal, de Telegram, de Wiebo, de Confide et de Cloackman en piratant les téléphones « intelligents » sur lesquels ces applications sont installées et de collecter les enregistrements audio et les messages avant que le cryptage ne soit activé », informe le document publié par WikiLeaks.

© FLICKR/ VIN CROSBIE
Espionnage en plein ciel: Air France dans le viseur des services secrets US et UK

Cette fuite a semé le trouble parmi les utilisateurs de WhatsApp, dont beaucoup ont réagi avec virulence aux nouvelles selon lesquelles l’application aurait commencé à partager des données avec Facebook l’année dernière.
La révélation de WikiLeaks suggère que les espions du gouvernement américain ont eu accès aux messages des utilisateurs malgré la mise en place d’un cryptage de bout en bout, qui est pourtant conçu pour protéger la confidentialité des utilisateurs.
Cependant, il se pourrait que la CIA n’ait pas piraté les applications elles-mêmes, mais craqué les outils de cryptage en attaquant les smartphones des utilisateurs.

© AFP 2017 SAUL LOEB
WikiLeaks publie plus de 8.700 documents concernant les capacités de cyber-espionnage de la CIA

Le site de Julian Assange, WikiLeaks, a annoncé le 7 mars la publication d’une nouvelle série de fuites sur la CIA sous le code « Vault 7 » qui sera, d’après le communiqué de l’organisation, la plus importante publication de documents confidentiels sur l’agence.
La première partie des fuites, intitulée « Year Zero », comprend 8 761 documents et fichiers qui ont été collectés sur un réseau isolé de haute sécurité du Centre Cyber Intelligence (département de la CIA) à Langley, dans l’État de Virginie.
Les fuites de « Year Zero » révèlent les capacités de piratage de la CIA contre un large éventail de produits américains et européens, notamment Windows, iPhone, Android et même les téléviseurs Samsung, qui ont été transformés en microphones cachés par le programme Weeping Angel…[lire la suite]

Réagissez à cet article

Source : *Les messages de WhatsApp peuvent être facilement lus par la CIA*

Le FBI pourra t-il accéder aux mails de Gmail ?

	Le FBI pourra t-il accéder aux mails de Gmail ?

Le juge fédéral Thomas Rueter de la cour de Philadelphie a donné son verdict et a statué concernant la saisie de mails depuis des serveurs étrangers, par les autorités américaines. Ce dernier a affirmé : «Même si la récupération de données électroniques par Google à partir de ses multiples centres de données à l'étranger peut en soi représenter un risque d'atteinte à la vie privée, la véritable atteinte intervient au moment de la divulgation aux Etats-Unis».

En gros, le juge fédéral a estimé que le fait d'ordonner à Google de remettre aux autorités les courriers électroniques de sa messagerie Gmail, stockés à l'étranger, n'était pas contraire à la loi. La firme de Mountain View devra se conformer aux mandats et perquisitions du FBI. Google a évidemment déclaré qu'il faisait appel de la décision, en se référant à la jurisprudence Microsoft, car une affaire similaire avait donné raison à Microsoft il y a quelques semaines à New York.

Google devra fournir au FBI les mails hébergés à l'étranger

Google ne souhaite pas livrer au FBI les e-mails stockés hors des Etats-Unis, afin de garantir la vie privée de ses usagers aux quatre coins du monde. Sont concernés par la décision du juge fédéral Thomas Rueter, les six serveurs de l'entreprise présents en Belgique, en Finlande, en Irlande, à Taïwan, Singapour et aux Pays-Bas.

Le juge a estimé qu' « *aucune ingérence significative* » avec les droits de propriété du titulaire du compte ne pouvait être invoquée concernant les données ciblées, car comme l'a fait remarquer le juge, Google procède déjà régulièrement au transfert de ces données vers ses serveurs aux Etats-Unis, pour ses propres business et sans que les clients en soient forcément informés. Thomas Rueter de la cour de Philadelphie a souligné : *« Ces transferts n'interfèrent pas avec l'accès du client ou les droits de propriété des données utilisateur. Même si le transfert interfère avec le contrôle du propriétaire du compte sur ses informations, cette interférence est minime et temporaire ».*

Il semble donc que le juge ait retourné les méthodes de Google contre lui-même pour justifier la légalité des saisies des e-mails stockés hors des Etats-Unis au FBI. Du côté de l'entreprise, on s'est contenté de déclarer : *« Nous continuerons à repousser les mandats excessifs ».*

Original de l'article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l'étranger

---

A Lire aussi :
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Original de l’article mis en page : Le FBI pourra bien accéder aux mails de Gmail situés à l’étranger