Ce qui changera après l’adoption du règlement général sur la protection des données

Ce qui changera après l’adoption du règlement général sur la protection des données

La Cnil a mis en ligne, le 15 juin dernier, une de ses synthèse qui facilitent, même pour les juristes, lappréhension intellectuelle dune nouvelle législation, en loccurrence le désormais célèbre « Règlement général sur la protection des données », puisque tel est le nom raccourci officiel du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à légard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (notre actualité du 4 mai 2016).

À très grands traits, selon la Cnil :

« La réforme de la protection des données poursuit trois objectifs :
• Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
• Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
• Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées. »
Source : « Règlement européen sur la protection des données : ce qui change pour les professionnels », Cnil, 15 juin 2016.
S'ensuit une série de chapitres présentant les diverses facettes des quelque 173 considérants et 99 articles du règlement ainsi décrypté :
• Un cadre juridique unifié pour l'ensemble de l'UE
• Un renforcement des droits des personnes
• Une conformité basée sur la transparence et la responsabilisation
• Des responsabilités partagées et précisées
• Le cadre des transferts hors de l'Union mis à jour
• Des sanctions encadrées, graduées et renforcées
• Comment les autorités de protection se préparent-elles ?

Peu de changements en vérité…

Signalons, pour ceux qui s'imagineraient que tout change puisque le nouveau règlement abroge toutes les lois de protection des données des États membres de l'Union, que les changements sont en fait fort peu nombreux et que le cadre de protection, surtout tel que nous le connaissions depuis la réforme de notre loi du 6 janvier 1978 sous l'influence de l'ancienne directive 95/46 CE, en date du 1er août 2004. Ce sont les mêmes fondements qui ont présidé à l'élaboration de ces règles communes, automatiquement insérés dans le droit national des États membres.

…Mais des changements piégeant à la marge

Mais cependant, il faut s'attendre à des changements, d'autant plus subreptices qu'ils interviennent dans un océan de stabilité.
On pourrait distinguer deux ordres de dispositions modificatrices :
• Les dispositions qui sont réellement nouvelles, comme par exemple, en France, la disparition des déclarations préalables à la Cnil et quelques autres dispositions vraiment nouvelles ;
• Les dispositions qui existaient déjà dans l'ancienne directive mais qui n'avaient pas été transposées dans la loi d'un pays membre. C'est par exemple le cas du droit à l'oubli dans la loi allemande.

Une marge de manœuvre résiduelle

Cependant, il reste dans le règlement, une certaine latitude d'action de la part des États membres. On peut le comprendre techniquement en comparant un règlement européen à une loi nationale, ce qu'il est effectivement. Il faut donc prendre en compte le fait que chaque pays pourra selon sa sensibilité prendre les mesures d'application de ce règlement – sous forme de décrets en France – ce qui aura de nouveau pour effet d'introduire des divergences de régime d'un pays à l'autre.

Article original de Didier Frochot

Réagissez à cet article

Original de l'article mis en page : Le règlement général sur la protection des données : ce qui change en Europe

---

Quelques chiffres sur les risques du WiFi public

Quelques chiffres sur les risques du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi *« un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec »*.

Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers *« intermédiaires »*, il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky,

Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires ignorent les risques du WiFi public

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Peut-on communiquer les données personnelles du défunt à ses ayants droit ?

Toute personne physique justifiant de son identité a le droit dobtenir la communication des données personnelles qui la concernent. En revanche, est exclue la communication de ces données aux ayants droit qui ne sauraient être regardés comme des « personnes concernées ».

Mme et MM. D., ayants droit de Mme E. D., décédée le 2 août 2012, ont demandé à la Banque de France, dernier employeur de la défunte, la communication du relevé des derniers appels téléphonique qu'elle avait passé avec le corps médical avant son décès.
Après le refus de la Banque de France, ils ont déposé une plainte le 1er février 2013 auprès de la Cnil.
La Cnil ayant confirmé le refus de la Banque de France dans une décision du 29 mai 2013, ils saisissent le tribunal administratif de Paris qui, par un jugement du 9 décembre 2014, a directement transmis cette requête au Conseil d'Etat.

Le Conseil d'Etat se prononce dans un arrêt du 8 juin 2016.
Il rappelle qu'aux termes du dernier alinéa de l'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, « la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».
En outre, aux termes de l'article 39 de cette même loi, « toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir (…) la communication, sous une forme accessible, des données à caractère personnel qui la concernent (…) ».
Ainsi, il résulte de ces dispositions qu'elles ne prévoient la communication des données à caractère personnel qu'à la personne concernée par ces données. C'est donc à bon droit que la présidente de la Cnil a pris la décision attaquée à l'égard de Mme et MM. D., qui ne pouvaient, en leur seule qualité d'ayants droit, être regardés comme des « personnes concernées ».
Article original de Céline Solomides

Réagissez à cet article

Original de l'article mis en page : Impossibilité de communiquer les données personnelles du défunt à ses ayants droit

Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

	Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

La Commission de l'Informatique et des Libertés (CIL) en partenariat avec les tribunaux du palais de justice de Ouagadougou, organise un séminaire de sensibilisation des magistrats et greffiers du palais de justice de Ouagadougou aux « enjeux de la protection des données personnelles et de la vie privée des citoyens à l'ère du numérique ». Ce séminaire se déroule à Ouagadougou ce mardi 28 juin 2016.

« Aucune personne n'est, de nos jours, à l'abri des actes cybercriminels, quel que soit son statut, son rang ou l'état de ses connaissances », a lancé Marguerite Ouédraogo/Bonané, présidente de la CIL. Si de nos jours la cybercriminalité avance à grand pas dans le monde entier, force est de constater que les initiatives pour l'affronter ne manquent pas. La lutte contre cette nouvelle forme de criminalité impose donc que de « nouvelles approches soient développées et que toutes ses dimensions soient maitrisées », a-t-elle reconnu. Dans l'optique de protéger les données des justiciables en justice, la CIL entend informer et sensibiliser les magistrats aux droits des personnes dont les données sont utilisées. « Notre mission aujourd'hui c'est de les informer et de les sensibiliser aux droits des personnes dont les données sont utilisées », a confié marguerite Ouédraogo/Bonané. A l'en croire, la protection des données couvre tout le territoire. Par conséquent, tous les Burkinabé sont concernés par cette protection. Elle révèle que ce séminaire ouvert aux magistrats permettra à ces derniers de protéger les données des justiciables comme le stipule « notre loi ».

Des communications qui seront faites dans ce séminaire

Plusieurs communications seront faites durant ce séminaire. En substance, une communication sera faite à l'intention des magistrats pour leur faire connaitre le cadre juridique et institutionnel des données personnelles au Burkina Faso. Une autre sera de leur faire connaitre la communication sur l'enquête judiciaire et la protection des données personnelles face à l'enquête judiciaire. Aussi, la formation sur l'utilisation de l'internet et des réseaux sociaux leur sera-t-elle donnée.

Vu l'importance de ce séminaire qui est focalisé sur les acteurs de la justice, Dieudonné Manly, Conseiller Technique du ministère de la justice, accorde un peu plus de crédit à l'ordre du jour quand il affirme qu' « aujourd'hui la cybercriminalité a pris de l'ampleur et il va falloir outiller les magistrats afin qu'ils puissent faire face à ce phénomène ». Aussi, pense-t-il que les thèmes choisis sont bien réfléchis et que ces thèmes vont, à son avis, « permettre aux magistrats de faire face à la cybercriminalité ».

Article original de Armand Kinda

Réagissez à cet article

Original de l’article mis en page : Lutte contre la cybercriminalité : les magistrats du palais de justice de Ouagadougou outillés pour en faire face

---

L’Etat français (ANSSI) va certifier les Cloud de confiance

L’Etat français (ANSSI) va certifier les Cloud de confiance

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.

L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « *Huit prestataires se sont lancés dans ce processus de qualification* », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « *La qualification n'est pas un outil de protectionnisme* », reprend Guillaume Poupart. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi.
Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 001.

Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +. Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : les Américains out ?

« *Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients* », explique Laurent Seror, le président d'Outscale, le fournisseur de Iaas né sous l'impulsion de Dassault Systèmes. « *Etant donné que nous sommes déjà certifiés ISO 27 001, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision* », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « *On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes.* »
La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Axelle Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « *Cet amendement n'était pas téléguidé*, assure aujourd'hui Guillaume Poupard. *Je l'ai découvert au moment des débats.* » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.
Article original de Reynald Fléchaux

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 du 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

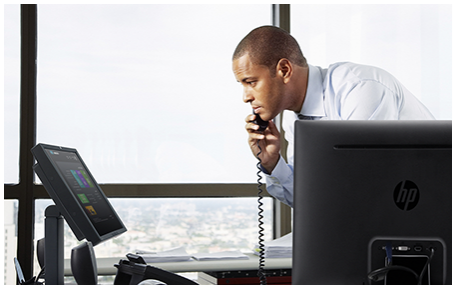
Original de l'article mis en page : L'Etat français va certifier les Cloud de confiance

---

Protection contre la Fuite des données, priorité pour les entreprises ?

Protection contre la Fuite des données, priorité pour les entreprises ?

Prévention des pertes de données des collaborateurs mobiles. Quand la mobilité oblige à la Data Loss Prevention.



La mobilité est à la fois un besoin et un défi pour les entreprises qui se battent pour créer une force de travail réellement fluide et entièrement digitale. Aujourd'hui, presque tous les collaborateurs travaillent avec un ou plusieurs périphériques mobiles contenant des informations d'entreprise, qu'il s'agisse d'un téléphone mobile, d'un ordinateur portable ou d'une tablette. L'un des premiers défis qui en découlent pour la direction informatique tient au fait que l'accès à distance aux données et aux e-mails se fait, par nature, « hors » du périmètre de l'entreprise, et qu'il est par conséquent très difficile de s'en protéger. La multitude des périphériques utilisés, en elle-même, complique la surveillance et le suivi des données d'entreprise consultées, partagées ou utilisées.

Data Loss Prevention : se concentrer sur les données

L'une des approches, choisie dans certaines entreprises, consiste à intégrer ces périphériques à une stratégie d'environnement de travail en BYOD. Les utilisateurs peuvent choisir le périphérique, le système d'exploitation et la version de leur choix, puisqu'il s'agit de leur propre périphérique. Malheureusement, cette approche peut en réalité créer des problèmes supplémentaires de sécurité et de DLP (prévention des pertes de données). En effet, de nombreux utilisateurs n'apprécient pas (voire interdisent) que leur employeur gère et/ou contrôle leur périphérique, pire encore, d'y installer des logiciels professionnels comme les programmes d'antivirus et de **VPN**.

Par conséquent, pour réussir, la stratégie de protection des données doit se concentrer sur la sécurisation des données uniquement, quel que soit le périphérique ou le mode d'utilisation. Dans un environnement d'entreprise, une grande majorité des données sensibles transitent dans les e-mails et leurs pièces jointes. Ainsi, une stratégie de protection des données réussie doit chercher à gérer et contrôler la passerelle par laquelle transitent les données, à savoir, ici, le compte d'e-mail d'entreprise.

Autre option : implémenter une suite d'outils de gestion de la sécurité mobile, ce qui permet de placer des mécanismes de sécurité sur la passerelle d'e-mail, et d'autoriser la création de règles de sécurité pour surveiller et contrôler la façon dont les informations d'entreprise sont traitées sur chaque périphérique.

Data Loss Prevention : Stratégie DLP tridimensionnelle

Une stratégie « DLP tridimensionnelle », surveille et contrôle le contenu transféré via un périphérique sur la base de critères précis. Par exemple, on peut limiter l'accès au contenu ou aux fichiers depuis le compte e-mail d'entreprise en fonction du pays, puisque les utilisateurs qui voyagent avec leur périphérique sont susceptibles d'accéder aux données et aux systèmes sur des réseaux Wi-Fi non sécurisés. Il est également possible de contrôler le contenu sur la base des mots clés qui figurent dans les e-mails (comme des numéros de sécurité sociale ou des numéros de contrat), afin d'interdire les pièces jointes ou le contenu incluant ce type d'information sur les périphériques mobiles. Comme les pièces jointes d'e-mail contiennent la majorité des informations sensibles transmises d'un périphérique à un autre, ce point est crucial lorsqu'il s'agit de protéger l'utilisation des périphériques dans l'environnement de travail. La troisième dimension est la surveillance du contexte, qui permet d'identifier et d'interdire le contenu pour des expéditeurs/destinataires spécifiques.

Ce type de considération permet de limiter les risques liés aux pertes de données et aux problèmes de sécurité pour cette partie des activités professionnelles Bien que cette approche ne suffise pas à contrôler et à sécuriser entièrement les banques de données d'une entreprise, la sécurité mobile va jouer un rôle de plus en plus vital pour la réussite des stratégies complètes de protection des données, au fur et à mesure que davantage de périphériques s'intègrent à nos habitudes de travail. (Par Eran Livne, Product Manager LANDESK)

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Data Loss Prevention – Data Security BreachData Security Breach

Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse » en Russie

Edward Snowden, l'ancien agent du renseignement américain réfugié en Russie, a dénoncé samedi 25 juin les lois antiterroristes adoptées par les députés russes. Ces dernières relèvent selon lui de « Big Brother » et de la « surveillance de masse », et a demandé qu'elles ne soient pas promulguées.

« La nouvelle loi russe Big Brother constitue une violation inapplicable et injustifiable des droits qui ne devrait jamais être promulguée », a écrit sur Twitter le lanceur d'alerte, qui a fui les Etats-Unis pour révéler l'ampleur de la surveillance menée par les services de renseignement américains.
« La surveillance de masse ne marche pas. Ce texte va coûter de l'argent et de la liberté à chaque Russe sans améliorer la sécurité », a-t-il insisté dans un second message.

Des lois extrêmement répressives

Adoptés vendredi lors de la dernière séance de la Douma (chambre basse) avant les législatives du 18 septembre, les projets de loi en question obligent en particulier les opérateurs de télécommunications et internet à stocker les messages, appels et données des utilisateurs pendant six mois pour les transmettre aux *« agences gouvernementales appropriées »* à leur demande.
Les réseaux sociaux se voient également obligés de stocker les données pendant six mois, selon l'un de ces textes qui doivent encore être approuvés par le Conseil de la Fédération (chambre haute) et promulgués par M. Poutine.
Ce délai de six mois *« n'est pas seulement dangereux, il est inapplicable »*, a prévenu M. Snowden, qui avait été critiqué, par le passé, pour ne pas critiquer assez sévèrement le régime de Vladimir Poutine.
Ces lois ont été dénoncées par l'opposition russe comme une tentative de *« surveillance totale »* de la part des autorités, mais aussi par les entreprises du numérique qui ont critiqué un coût exorbitant.
Elles introduisent par ailleurs des peines de prison pour la non-dénonciation d'un délit, abaissent l'âge de la responsabilité pénale à 14 ans et introduisent des peines allant jusqu'à sept ans de détention pour la*« justification publique du terrorisme »*, y compris sur internet.
Article original Le Monde

Réagissez à cet article

Original de l'article mis en page : Russie : Edward Snowden dénonce une loi « Big Brother » et la « surveillance de masse »

Que change le brexit pour la protection des données personnelles ?

	Que change le brexit pour la protection des données personnelles ?

Le nouveau règlement européen sur les données personnelles, qui doit entrer en vigueur en mai 2018, ne s'appliquera peut-être jamais au Royaume-Uni. Le pays devrait, une fois sorti, conserver sa propre législation, basée sur les directives européennes antérieures. Cela pourrait obliger le Royaume-Uni à conclure un accord spécifique avec l'UE à 27, sous peine de se voir infliger des restrictions dans le transfert de données avec les pays de l'UE.

Le Royaume-Uni se retrouverait ainsi dans la même position que lesEtats-Unis, dont l'accord avec l'UE (Safe Harbor) a été remis en cause à l'automne pour être remplacé par le Privacy Shield, qui devrait entrer en vigueur cet été. L'adhésion à ces accords conditionne la possibilité de transférer des données personnelles de citoyens de l'UE aux Etats-Unis.
Si le Safe Harbor a été remis en cause, c'était notamment à cause des questions de surveillance de masse aux Etats-Unis. Soit le Royaume-Uni choisit de se rapprocher du modèle américain sur les questions de surveillance et de données personnelles, soit il se cale sur les standards européens.
Dans le premier cas, il faudrait que les grandes entreprises américaines (Google, Apple, Facebook, Microsoft…), dont la plupart des datacenters sont à Dublin, en Irlande, les rapatrient au Royaume-Uni, comme le note le site de la radio publique irlandaise RTE. La présence de ces datacenters en Irlande doit rassurer les Européens, puisque l'Irlande, elle, n'est pas concernée par le Brexit. Ce sont donc les standards européens qui s'appliquent.
Avant la sortie effective, rien ne change. « A moyen terme, les choses vont rester très stables. Le Royaume-Uni met en oeuvre la directive européenne sur les données personnelles depuis plus de 20 ans. La suite dépendra des accords qui seront négociés entre le Royaume-Uni et l'UE. Le cadre réglementaire ne changera donc pas pendant un bon bout de temps », assure à L'Express Daniel Kadar, avocat associé au cabinet Reed Smith.
Article original de Raphaële Karayan

Réagissez à cet article

Original de l’article mis en page : Ce que le Brexit va changer pour les géants du Web – L’Express L’Expansion

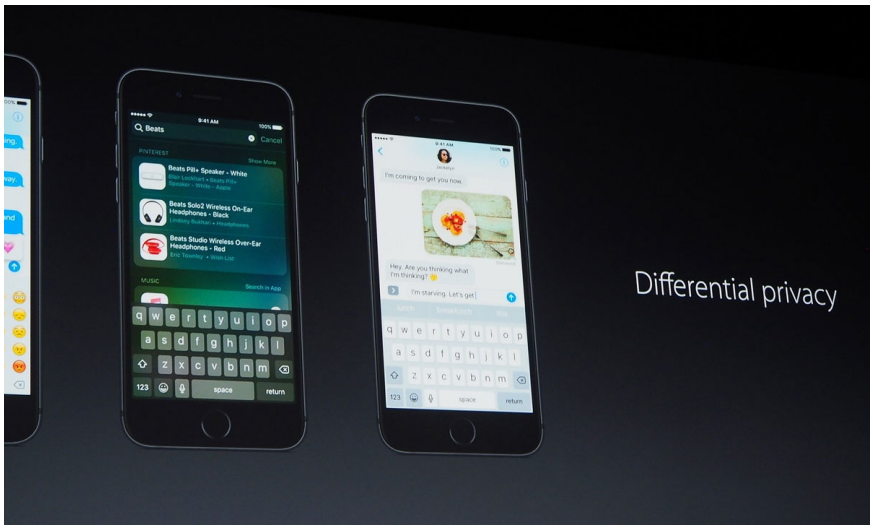
---

Finalement Apple collectera des données personnelles, avec votre accord

Finalement Apple collectera des données personnelles, avec votre accord

---

Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.



Point d'achoppement et de différence avec Google, Facebook et autres, votre vie privée et les données qui y sont associées sur vos appareils n'intéressent pas Apple.
Jusqu'alors, Apple s'est toujours refuser à accéder ou collecter vos données.
Cependant les nouvelles fonctionnalités de suggestion et d'identification d'iOS 10 ne peuvent se prétendre pertinentes sans avoir accès à un minimum de données !
Les techniques de « differential privacy » mises en oeuvre pour iOS 10 ne permettront pas une identification de l'utilisateur qui fournit ses données mais Apple, selon Recode, vous- demandera votre accord avant d'attaquer toute collecte d'information.
Dans un premier temps, le type de données collectées sera limité à quatre domaines :
– les nouveaux mots ajoutés au dictionnaire personnel d'iOS,
– les émoticônes utilisées,
– les liens profonds marqués comme public dans les applications,
– les suggestions de recherche dans les notes.
Pour ne pas rater le train de l'intelligence artificielle, Cupertino ne pouvait pas rester à l'écart d'une forme de collecte et d'exploitation de données. Cependant, ne souhaitant pas en faire directement commerce ni renier ses grands principes, Apple se doit de naviguer entre deux eaux et d'innover dans ce domaine.
On est encore loin de la façon de procéder de compagnies comme Google et Facebook !
Article original de bpepermans

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

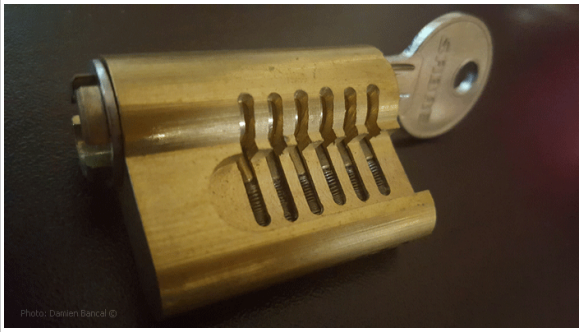
Réagissez à cet article

Original de l’article mis en page : Finalement Apple collectera des données personnelles, avec votre accord | Slice42

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Vol de ses données personnelles – Plusieurs sources ont révélé récemment la mise en vente sur le web de plus de 117 millions de profils d'utilisateurs LinkedIn dérobés en 2012. Ce type d'actualité rappelle que personne n'est à l'abri d'un vol de ses données personnelles qui risquent d'être utilisées à des fins illicites. Cette question est d'autant plus cruciale à l'heure où le nombre de logiciels malveillants, ransomwares et autres virus explose. Aujourd'hui, 67 % des Français sont soucieux quant à la protection de leurs informations personnelles sur internet et 83 % d'entre eux sont hostiles à la conservation de ces données (Source : Institut CSA).



Malgré cette méfiance, dans un monde où l'utilisation d'Internet est devenue omniprésente, les utilisateurs ont tendance à exposer très facilement leur vie privée et leurs données personnelles – parfois par paresse ou par mégarde, mais souvent par manque d'information. Il existe cependant des moyens simples et efficaces de limiter ces risques.
Michal Salat, Threat Intelligence Manager chez Avast, commente : « ***Les sphères privées et professionnelles se fondent de plus en plus, poussant fréquemment les utilisateurs à accéder à leurs plateformes de travail depuis des terminaux personnels ou à utiliser leurs appareils professionnels à la maison par exemple. Or, en adoptant ces comportements, les internautes exposent davantage leurs données personnelles.***«

Vol de ses données personnelles
Pour éviter que cela n'arrive, les utilisateurs doivent d'abord se protéger des menaces extérieures à leur appareil en commençant par créer un mot de passe ou un code PIN sur les écrans et les applications mobiles, limitant ainsi l'accès aux données en cas de perte ou de vol. Mais encore faut-il qu'il soit suffisamment compliqué pour ne pas être déchiffré trop facilement. C'est pourquoi il est recommandé d'utiliser des mots de passes complexes – combinant lettres, chiffres, caractères spéciaux et majuscules – et qui ne reprennent pas non plus des informations personnelles facilement accessibles en ligne, telle que la date de naissance ou le prénom de ses enfants. Il est également important de changer ses codes régulièrement.
Il faut garder en tête que les cybercriminels sont à l'affût de la moindre faille à exploiter pour récolter des gains et cherchent très souvent à récupérer des informations bancaires. C'est pourquoi les internautes doivent à tout prix éviter de sauvegarder leurs coordonnées bancaires dans leurs terminaux, quels qu'ils soient. A titre d'exemple, beaucoup d'utilisateurs PayPal ont perdu de grosses sommes d'argent lorsque des hackers ont réussi à se connecter à leurs PC via un compte TeamViewer piraté et se sont servi des identifiants enregistrés pour transférer l'argent depuis les comptes PayPal.

Les pirates parviennent à créer des e-mails d'hameçonnage très sophistiqués notamment grâce à la collecte d'informations personnelles publiques disponibles sur le web – accessibles sur les réseaux sociaux par exemple. Il est alors essentiel pour l'utilisateur de poster le moins d'informations possibles sur Internet ou de s'assurer que celles-ci sont en mode privé. Il est également crucial de supprimer ses comptes s'ils ne sont plus utilisés, car bien qu'abandonnés, ces profils restent en ligne et des personnes malintentionnées pourraient usurper l'identité de l'internaute ou nuire à sa réputation en ligne en utilisant des informations sensibles contre lui.
La protection de la vie privée et des données personnelles (vol de ses données personnelles) implique une modification du comportement des internautes à commencer par de meilleures méthodes de gestion de mots de passe, une vigilance accrue sur leur utilisation d'Internet et des informations personnelles partagées publiquement – comme sur les réseaux sociaux. Au-delà des bonnes pratiques, il existe des solutions qui répondent aux problématiques liées à la vie privée. Cependant face aux menaces, il n'appartient qu'à nous de nous discipliner et de tout mettre en œuvre pour protéger nos données personnelles.

Article original de Damien Bancal

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 : Devenir maître dans l'art de protéger sa vie privée sur le net – Data Security BreachData Security Breach