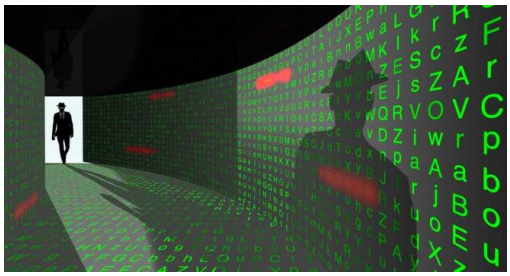
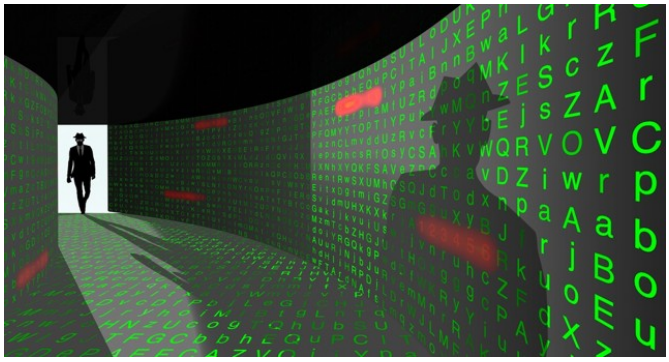
Combien vous coûterait le piratage de vos données ?



Combien vous coûterait le piratage de vos données ?

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.



Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

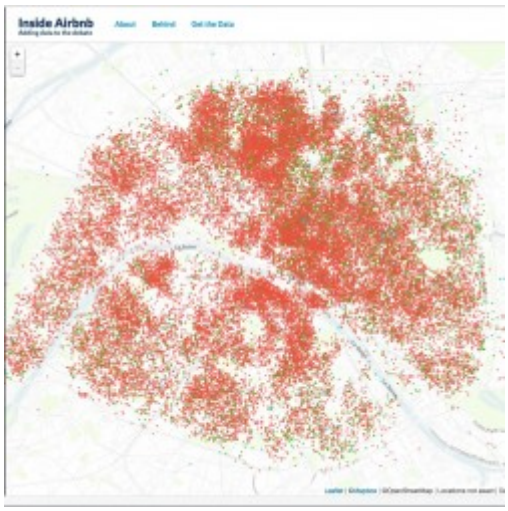
EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Dénoncez les hôtes Airbnb, Paris vous le rendra…



Dénoncez les hôtes Airbnb, Paris vous le rendra…

La mairie de Paris appelle les voisins à dénoncer les hôtes Airbnb non déclarés aux services municipaux.

Dans le dernier chapitre d'une bataille en cours sur l'économie de partage en France, la ville de Paris demande aux résidents de dénoncer leurs voisins qui ne sont pas correctement enregistrés comme meublé ou hôte du site Airbnb.
Selon le site Europe1.fr, les services municipaux ont créée une nouvelle section sur le portail open data de la ville qui répertorie les résidents qui se sont inscrits comme un hôte Airbnb. 126 résidences sont aujourd'hui listées comme locations saisonnières sur la plate-forme Airbnb alors que le site revendique plus de 41 000 logements (35 185 appartements et 5 827 chambres). Paris serait une des destinations les plus populaires sur sa plate-forme selon Airbnb. Et avec la carte publiée par la ville de Paris, il est facile de repérer les hôtes en règle, c'est à dire qui auront déclarés ces revenus et encaissés la taxe de séjour reversée ensuite à la mairie. C'est une des batailles engagées depuis plusieurs mois par les hôteliers qui crient à la concurrence déloyale. La ville de Berlin a également engagé un bras de fer avec Airbnb pour limiter les locations de meublés sur la plate-forme.

Dans une interview avec Europe1, Mathias Vicherat, chef de cabinet pour le maire de la ville, indique espérer que les résidents utiliseront les informations sur le portail de données ouvertes pour faire pression sur leurs voisins qui ne respectent pas les règles. Les hôtes Airbnb en violation avec les règlements de la ville pourraient faire face à une amende de 25 000€ s'ils louent plus de quatre mois par an leurs logements à des touristes. « On souhaite que cela provoque un espèce de choc de conscience de civisme, et que les gens se mettent en règle d'eux-mêmes, sans attendre d'être éventuellement signalé par un de leurs voisins », dit-il. La mairie explique qu'il n'est pas question d'appeler à la dénonciation comme durant la Seconde Guerre Mondiale où cinq millions de lettres anonymes avaient été envoyées à la police ou la Gestapo… [Lire la suite]

Réagissez à cet article
Article de Serge Leblal

Source : *Paris incite ses habitants à dénoncer les hôtes Airbnb – Le Monde Informatique*

Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach

	Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

La directive européenne de protection des données personnelles est morte ! Vive le règlement général sur la protection des données (GDPR). Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

En 1995, l'Europe s'équipait de la directive européenne de protection des données personnelles. Mission, protéger les informations des utilisateurs d'informatique. 21 ans plus tard, voici venir le règlement général sur la protection des données (GDPR). La Commission européenne avait proposé en 2012 un nouveau règlement portant sur un ensemble de règles unique pour toutes les données collectées en ligne afin de garantir qu'elles soient conservées de manière sûre et de fournir aux entreprises un cadre clair sur la façon dont les traiter.

Mercredi 13 avril 2016, le paquet législatif a été formellement approuvé par le Parlement dans son ensemble. Le GDPR impose aux entreprises (petites ou grandes) détenant des données à caractère personnel d'alerter les personnes touchées par une fuite, une perte, un piratage de la dire informations privée.

Grand groupe, PME, TPE doivent informer les autorités de contrôle nationales (CNIL) en cas de violation importante de ces données.
Comme je pouvais déjà vous en parler en 2014, il faut alerter les autorités dans les 72 heures après avoir découvert le problème. Les entreprises risquent une grosse amende en cas de non respect : jusqu'à 4% de son chiffre d'affaire. Les informations que nous fournissons doivent être protégées par défaut (Art. 19). A noter que cette régle est déjà applicable en France, il suffit de lire le règlement de la CNIL à ce sujet. Faut-il maintenant que tout cela soit véritablement appliqué.

Fuite, perte, piratage de données
Parmi les autres articles, le « 7 » indique que les entreprises ont l'obligation de demander l'accord « *clair et explicite* » avant tout traitement de données personnelles. Adieu la case par défaut imposée, en bas de page. De l'opt-in (consentement préalable clair et précis) uniquement. Plus compliqué à mettre en place, l'article 8. Je le vois dans les ateliers que je mets en place pour les écoles primaires et collèges. Les parents devront donner leur autorisation pour toutes inscriptions et collectes de données. Comme indiqué plus haut, les informations que nous allons fournir devront être protégées par défaut (Art. 19). Intéressant à suivre aussi, l'article 20. Comme pour sa ligne téléphonique, le numéro peut dorénavant vous suivre si vous changez d'opérateur, cet article annonce un droit à la portabilité des données. Bilan, si vous changez de Fournisseur d'Accès à Internet par exemple, mails et contacts doivent pouvoir vous suivre. L'histoire ne dit pas si on va pouvoir, du coup, garder son adresse mail. 92829@orange.fr fonctionnera-t-il si je passe chez Free ?
La limitation du profilage par algorithmes n'a pas été oublié. En gros, votre box TV Canal +, Orange ou Netflix (pour ne citer que le plus simple) utilisent des algorithmes pour vous fournir ce qu'ils considèrent comme les films, séries, émissions qui vous conviennent le mieux. L'article 21 annonce que l'algorithme seul ne sera plus toléré, surtout si l'utilisateur n'a pas donné son accord.
Enfin, notre vie numérique est prise en compte. Les articles 33 et 34 s'annoncent comme les défenseurs de notre identité numérique, mais aussi notre réputation numérique. L'affaire Ashley Madisson est un des exemples. Votre identité numérique est volée. L'entreprise ne le dit pas. Votre identité numérique est diffusée sur Internet. Vous ne la maîtrisez plus.
Bref, 33 et 34 annonce clairement que les internautes ont le droit d'être informé en cas de piratage des données. La CNIL sera le récipiendaire des alertes communiquées par les entreprises piratées. Bref, fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !
Les entreprises ont jusqu'au 1er janvier 2018 pour se mettre en conformité. Les 28 pays membres doivent maintenant harmoniser leurs lois sur le sujet. Je me tiens à la disposition des entreprises, associations, particuliers qui souhaiteraient réfléchir à leur hygiène informatique.

Police : nouvelles règles sur les transferts de données
Le paquet sur la protection des données inclut par ailleurs une directive relative aux transferts de données à des fins policières et judiciaires. La directive s'appliquera aux transferts de données à travers les frontières de l'UE et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre.
Les nouvelles règles ont pour but de protéger les individus, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et limites clairs en matière de transferts de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales – incluant des garanties et des mesures de prévention contre les menaces à la sécurité publique, tout en facilitant une coopération plus aisée et plus efficace entre les autorités répressives.

« ***Le principal problème concernant les attentats terroristes et d'autres crimes transnationaux est que les autorités répressives des États membres sont réticentes à échanger des informations précieuses*** », a affirmé Marju Lauristin (S&D, ET), députée responsable du dossier au Parlement.
« ***En fixant des normes européennes sur l'échange d'informations entre les autorités répressives, la directive sur la protection des données deviendra un instrument puissant et utile pour aider les autorités à transférer facilement et efficacement des données à caractère personnel tout en respectant le droit fondamental à la vie privée***« , a-t-elle conclu… [Lire la suite]

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

- Expertise techniques et judiciaire en litige commercial, piratages, arnaques Internet;
- Expertise de systèmes de vote électronique;
- Formation en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Suivez nous sur

Réagissez à cet article

Source : *Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach*

ZATAZ 93 millions d'électeurs Mexicains accessibles sur la toile – ZATAZ

93 millions d'électeurs Mexicains accessibles sur la toile

Accessibles sur la toile ! Cela n'arrive pas qu'aux autres, la preuve, une fois de plus. Une base de données mal configurée a permis d'accéder à 93,4 millions de données d'électeurs mexicains. Une BDD sauvegardée… aux USA !

Dans la série, le #Fail du jour, voici venir le Mexique et des données accessibles sur la toile ! Il y a peu, une base de données énorme a été volée à la Turquie, 49 millions de dossiers, et d'une seconde, de 55 millions d'informations d'électeurs Philippins.
Aujourd'hui, traversons l'Atlantique et allons regarder du côté des électeurs Mexicains. Plus de 93,4 millions de citoyens mexicains ont eu leurs modalités d'inscription sur les listes électorales diffusées sur la toile via une base de données mal configurée. C'est Chris Vickery, chercheur en sécurité informatique qui a découvert la chose via l'outil Shodan et le bug de configuration visant le gestionnaire de base de données MongoDB.
Plus étonnant, la base de données qui appartient à l'Instituto Nacional Electoral (INE), une BDD de 132 Go, étaient sauvegardées aux USA, chez Amazon.
Parmi les informations accessibles détectées par Chris Vickery : identités, filiation familiale, enfants, métier, adresse postale, numéro d'identité, numéro d'électeur…

Accessibles sur la toile
Bref, à force de nous vendre le cloud comme notre nouvel ami (écologique, peu couteux, friendly), c'est surtout nous faire oublier que le cloud, c'est le diable en 2.0.
Cette année, La Grèce, Israël, les Etats-Unis, les Philippines et la Turquie se sont vues confrontées avec la fuite des données de leurs ressortissants. A ce rythme là, le big data de la NSA et autres collecteurs discrets n'est pas prêt de se tarir !… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ 93 millions d’électeurs Mexicains accessibles sur la toile – ZATAZ*

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

---

Le nouveau règlement européen relatif à la protection des données personnelles (GDPR) fait grand bruit en Europe. Il donne, en effet, plus de droits aux consommateurs sur la façon dont leurs données sont traitées et requiert des contrôles complémentaires (et des informations) sur quiconque dispose de données personnelles dans l'Union européenne.

Comme toutes les lois, celle-ci a été largement discutée, avec des points de vue contradictoires, mais une chose a été acceptée par tous : les entreprises auront deux ans, à compter de la date de publication de la loi (en juin 2016), avant que celle-ci entre en vigueur. Deux années indispensables aux entreprises pour leur permettre de mettre en place les politiques, les processus et les technologies nécessaires pour être en conformité avec le règlement.
En avance sur ses voisins européens, la France a d'ores et déjà adopté un projet de loi en phase avec les principes fondamentaux du règlement européen relatif à la protection des données personnelles. Ainsi, le projet de loi pour une République numérique, validé par l'Assemblée nationale le 26 janvier dernier (actuellement examiné par le Sénat), devrait être approuvé pour entrer en vigueur cette année.

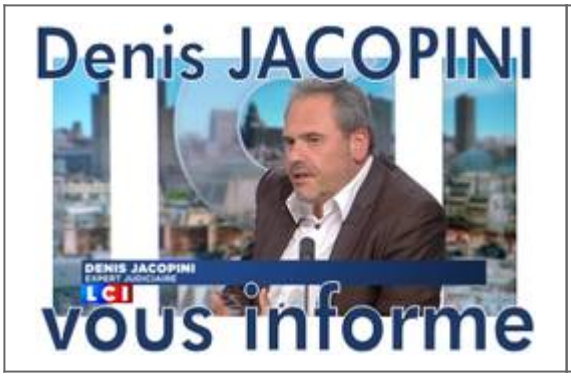
Quelles sont les grandes lignes de la loi pour la République numérique ?

Droit à la portabilité des données : le consommateur peut demander à ce que ses données soient conservées par le responsable du traitement des données et dispose en toutes circonstances d'un droit de récupération de ses données.
• Conservation des données : le responsable du traitement des données doit informer le consommateur de la durée pendant laquelle les données sont conservées.
• Droit de rectification : les consommateurs peuvent demander à ce que leurs données soient éditées pour les modifier.
• Droit à la suppression : les personnes concernées peuvent demander à ce que leurs données soient supprimées ou interdire l'usage de leurs données.
• Recours collectifs : les consommateurs peuvent déposer une plainte collective pour demander réparation lors de la perte ou de l'utilisation abusive de leurs données.
• Amende maximale : celle-ci peut aller de 150.000 à 20.000.000 euros ou 4 % du chiffre d'affaires global, pour l'amende la plus élevée.
D'autres pays vont-ils prendre exemple sur la France pour faire avancer leurs propres législations sur la protection des données avant la mise en œuvre du règlement européen ? Il y a fort à parier que oui. Et les entreprises ont également anticipé cette nouvelle réglementation puisque l'utilisation de services cloud basés dans la zone européenne a presque doublé en six mois (de 14,3 % au premier trimestre 2015 à 27 % pour 2016)… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur les données personnelles : la France en avance sur ses voisins européens – Global Security Mag Online*

Le Paquet « Protection des données à caractère personnel » adopté



Le Paquet « Protection des données à caractère personnel » adopté

Le règlement général sur la protection des données ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives ont été adopté le 14 avril…

Ce Paquet vise à réformer la législation communautaire d'une part et à remplacer la directive générale sur la protection des données qui datait de 1995 d'autre part.

1. Les nouveaux principes à mettre en oeuvre par le règlement

Le règlement européen sur la sur la protection des données (2) consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés.
Si les formalités administratives sont simplifiées pour mettre en œuvre un traitement, les obligations sont en revanche renforcées pour assurer une meilleure protection des données personnelles :

• la démarche de « Privacy by design » (respect de la protection des données dès la conception) (Règlement, art. 25 §1) ;
• la démarche de « Security by default » (sécurité par défaut) (Règlement, art. 25 §2) ;
• les règles d'accountability (obligation de documentation) (Règlement, art. 24) ;
• l'étude d'impact avant la mise en œuvre de certains traitements (Règlement, art. 35) ;
• la désignation obligatoire d'un Data Protection Officer (DPO) (Règlement, art. 37) ;
• les nouveaux droits fondamentaux des personnes (droit à l'oubli, droit à la portabilité des données, etc.) sur lesquels nous reviendrons dans un prochain article.

1.1 Le respect de la protection des données dès la conception ou « Privacy by design »

Le règlement européen sur la protection des données consacre le principe de « Privacy by design » qui impose aux entreprises publiques comme privées de prendre en compte des exigences relatives à la protection des données dès la conception des produits, services et systèmes exploitant des données à caractère personnel.
Cette obligation requiert que la protection des données soit intégrée par la Direction des systèmes d'information dès la conception d'un projet informatique, selon une démarche « Privacy by design ». Elle rend également nécessaire la coopération entre les services juridiques et informatiques au sein des entreprises
.

1.2 La sécurité par défaut ou « Security by default »

Le règlement européen sur la protection des données pose une nouvelle règle, la « sécurité par défaut ». Cette règle impose à tout organisme de disposer d'un système d'information ayant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes (enregistrement, exploitation, administration, intégrité et mise à jour).
La sécurité du système d'information doit être assurée dans tous ses éléments, physiques ou logiques (contrôle d'accès, prévention contre les failles de sécurité, etc.).
Par ailleurs, cette règle implique que l'état de la sécurité du système d'information puisse être connu à tout moment, par rapport aux spécifications du fabricant, aux aspects vulnérables du système et aux mises à jour.

1.3 L'étude d'impact

Le règlement européen sur la protection des données consacre l'obligation par les organismes de réaliser des analyses d'impact relatives à la protection des données.
Cette obligation impose à tous les responsables de traitements et aux sous-traitants d'effectuer une analyse d'impact relative à la protection des données personnelles préalablement à la mise en œuvre des traitements présentant des risques particuliers d'atteintes aux droits et libertés individuelles.
Dans un tel cas, le responsable du traitement ou le sous-traitant, doit examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et apporter la preuve que le règlement sur la protection des données est bien respecté.

1.4 L'obligation de documentation ou « accountability »

Le règlement européen sur la protection des données met à la charge du responsable de traitement des règles d'accountability qui constituent la pierre angulaire de la conformité « ab initio » avec la règlementation en matière de données personnelles.
Il s'agit pour le responsable du traitement de garantir la conformité au règlement en adoptant des règles internes et en mettant en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.
Les mesures prévues en matière de données personnelles et d'accountability vont de la tenue de la documentation, à la mise en œuvre des obligations en matière de sécurité en passant par la réalisation d'une analyse d'impact.
Cette démarche anglo-saxonne connue sous le terme d'accountability est une obligation pour le responsable du traitement de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues du règlement.
Il devra démontrer qu'il a rempli ses obligations en matière de protection des données. C'est une charge de la preuve qui l'oblige à documenter l'ensemble des actions de sa politique de protection des données de manière à pouvoir démontrer aux autorités de contrôle ou aux personnes concernées comment il s'y tient.

2. La protection des données à caractère personnel traitées à des fins répressives

Les pratiques en matière pénale sont très différentes d'un Etat à l'autre. Jusqu'à présent il n'y avait pas de cadre commun aux services répressifs des Etats membres.
La directive relative à la protection des données à caractère personnel à des fins répressives (3) prévoit que chaque Etat membre doit suivre un cadre commun tout en développant sa propre législation qui devra reprendre toutes les règles de base en matière de protection des données notamment en matière de sécurité.
Ce n'est pas une chose aisée dans la situation actuelle avec les menaces terroristes qui pèsent en Europe.
Parmi les nouveaux éléments importants de cette directive, figure la nécessiter de se préoccuper en permanence de la protection des données et de la vie privée. A ce titre, toutes les institutions liées aux services répressifs devront se doter d'un « Data protection officer ».
Il ne devrait plus y avoir de collecte de données personnelles sans objectif clair, sans durée limitée et les justiciables auront des droits clairs, comme celui de savoir quelles sont les données collectées, à quelle fin, et combien de temps elles seront conservées.
La directive permet de prendre en compte les spécificités liées aux services répressifs tout en préservant les droits universels des citoyens justiciables. Ces deux textes font partis d'un même paquet « protection des données ».
La tâche n'a pas été simple de réformer la directive de 1995 et d'en faire un règlement unifié directement applicable par les Etats membres. C'est probablement une grande première que d'avoir réalisé un tel texte qui s'applique directement à toute l'Union européenne dans un domaine qui règlemente un droit aussi fondamental que la protection des données.
Le règlement entrera en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne. Ses dispositions seront directement applicables dans tous les Etats membres deux ans après cette date, soit en avril 2018.
En ce qui concerne la directive relative à la protection des données à caractère personnel à des fins répressives, les Etats membres auront deux ans pour transposer les dispositions qu'elle contient dans leur droit national.
Il s'agit là d'une grande avancée pour l'Union européenne tant pour les citoyens consommateurs que pour les entreprises.
Notes :
(1) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption du règlement général sur la protection des données.
(2) Règlement général sur la protection des données révisé le 8 avril tel qu'adopté par le Parlement européen le 14 avril 2016.
(3) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption de la directive relative à la protection des données à caractère personnel à des fins répressives… [Lire la suite]

Réagissez à cet article

Source : *Adoption du Paquet « Protection des données à caractère personnel »*

Microsoft poursuit le gouvernement américain

Microsoft	Microsoft poursuit le gouvernement américain

Aux États-Unis, Microsoft a initié une procédure à l'encontre du Department of Justice afin de faire invalider certaines dispositions de l'Electronic Communications Privacy Act. En substance, le géant veut pouvoir prévenir ses clients quand les autorités réclament des données les concernant.

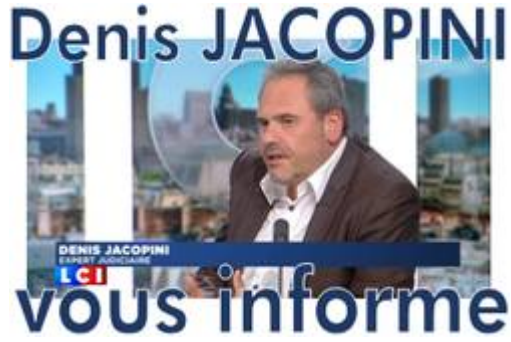
Au fil des 18 derniers mois, Microsoft a reçu 5 624 demandes d'information émanant des autorités. Sur ce total, la firme a compté la bagatelle de 2 576 requêtes associées à une obligation de garder le silence. Elle a en outre relevé 1 752 cas dans lesquels cette contrainte était valable jusqu'à nouvel ordre – autant dire ad vitam æternam. Pour Microsoft, cette situation n'est pas acceptable. Sous couvert de l'Electronic Communications Privacy Act, établi en 1986, les autorités ignorent complètement la Constitution. Une procédure légale vient donc d'être engagée.
Concrètement, Microsoft s'attaque au Department of Justice (équivalent de notre ministère de la Justice), à qui il reproche d'ignorer sciemment deux amendements de la Constitution. En empêchant la firme de prévenir un client lorsque ses données sont consultées par une agence du gouvernement, celui-ci ferait à la fois fi de la liberté d'expression de Microsoft (1er amendement de la Constitution) et du droit du client à savoir ce que les autorités font avec sa propriété (4e amendement). En conséquence, plusieurs dispositions de l'Electronic Communications Privacy Act devraient tout simplement être invalidées. Reste à voir si le tribunal de Washington partagera ce point de vue.

Rappelons que ce n'est pas la première initiative de Microsoft pour mettre un terme aux indiscrétions silencieuses de la NSA (entre autres). Cela fait deux ans, maintenant, que la firme réclame ouvertement une très sérieuse remise en question des pratiques du gouvernement et des différents corps policiers qui en dépendent. L'appel, cependant, n'a toujours pas porté le moindre fruit. Il est donc temps, à l'évidence, d'actionner d'autres leviers pour espérer aboutir à un résultat… [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : Microsoft poursuit le gouvernement américain*

Que deviendront nos données personnelles après notre mort ?

	Que deviendront nos données personnelles après notre mort ?

Après la disparition d’un proche, peut-on récupérer les fichiers, les achats réalisés par celui-ci ?

3 milliards d’êtres humains sont aujourd’hui connectés à Internet, échangeant de nombreuses données. Mais que deviennent celles-ci après la mort ? En France, plus de 85% de la population sont ainsi connectés. Réseaux sociaux, messagerie, photos… D’innombrables données personnelles numériques sont échangées.

Bientôt une loi sur les données numériques

Les personnes interrogées ne savent pas ce qu’elles deviennent. Depuis 40 ans, un texte interdit à quiconque de consulter ou de porter atteinte aux informations personnelles. C’est la protection des données qui, de facto, s’est étendue au numérique. « La protection des données personnelles stipule qu’un tiers n’a pas le droit d’accéder aux données sauf en cas de force majeure ou sous mandat d’un juge », explique Gilbert Kallenborn, du site zero1net.com.

Aujourd’hui, on stocke photos et messages tout au long de notre vie, des souvenirs auxquels les héritiers aimeraient avoir accès. Pour y arriver, les sénateurs préparent une nouvelle loi. Un internaute pourra indiquer des directives à suivre après sa mort : une personne de son choix pourra fermer les comptes et récupérer leurs données. A défaut, ses héritiers légaux s’en chargeront. Pour être vraiment sûr de l’avenir de ses données, ne reste qu’une garantie : le testament. La nouvelle loi sera débattue au parlement avant l’été… [Lire la suite]

Réagissez à cet article

Source : *Internet : que deviennent nos données personnelles après notre mort ?*

CNIL, un nombre record de plaintes en 2015

CNIL, un nombre record de plaintes en 2015

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

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

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

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

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

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

C'est nouveau ! A suivre …

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

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

Des demandes de droit d'accès indirect toujours en hausse

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Le renseignement et la lutte contre le terrorisme

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

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

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

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

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

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

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

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

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

En Europe

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

Réagissez à cet article