La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas)

La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas)

Alors qu'il s'apprête à lancer de la publicité ciblée hors de ses services, y compris auprès des non-utilisateurs de sa plateforme, Facebook a obtenu un sursis de 3 mois de la Cnil. L'autorité lui reproche une collecte déloyale de données personnelles.

Le réseau social a été mis en demeure le 9 février par l'autorité française de protection des données personnelles. La Cnil reproche à Facebook une collecte déloyale de données de navigation d'internautes non membres et l'absence de recueil d'un consentement pour le croisement de données à des fins publicitaires.
La firme de Mark Zuckerberg disposait d'un délai de trois mois pour se mettre en conformité. Mais d'après le JDN, Facebook a sollicité auprès de la Cnil un délai supplémentaire de trois mois. Celui-ci lui a été accordé.

Sécurité et publicité grâce au même cookie finalement

« Nous avons repoussé au 9 août le délai obligatoire pour se mettre en conformité » répond la Cnil. Sur le plan commercial, Facebook se montre plus dynamique. La société a annoncé tout récemment un changement de cap.
Elle entend en effet proposer de la publicité ciblée à tous les internautes et non uniquement à ceux inscrits sur son réseau. Pour suivre ces internautes,Facebook met à profit son cookie Datr. La firme assurait pourtant jusqu'à présent que ce cookie avait pour seule finalité la sécurité.
Plus d'ambiguïté à présent. Le réseau social précise que sa régie publicitaire, Audience Network, suivra dorénavant l'ensemble des internautes via ses cookies « même ceux qui ne disposent pas de compte Facebook ou ne s'y connectent pas. »… [Lire la suite]
Merci à ZdNet

Réagissez à cet article

Source : *La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas) – ZDNet*

ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ

	**Fuites de données de Santé en France**

Santé et fuite de données – Plus de 200 millions de dossiers médicaux de ressortissants américains ont disparu depuis 2015. Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Le Parlement européen a adopté le jeudi 14 avril 2016 le règlement européen sur la protection des données. Le règlement qui sera applicable à partir du 25 mai 2018 dans l'ensemble des pays membres de l'Union européenne. Avec cette jolie annonce que l'on attend depuis des années, je me suis penché sur un cas concret de fuites de données : les dossiers médicaux. A la fin de ma compilation et analyses des datas collectées, ma question est la suivante : Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Santé et fuite de données : Plus de 200 millions de dossiers médicaux perdus en 1 an

J'ai analysé les établissements de santé américains. Il faut dire que cela est plus simple. La France n'a aucun moyen de contrôle au sujet des fuites d'informations dans le secteur Français de la santé. Et ce n'est pas faute d'avoir des personnes très compétentes au Ministère de la Santé et des Affaires Sociales. Mais en France, pour le moment, aucune obligation n'est faite pour que les patients soient alertés en cas de fuite, de piratage, de perte de leurs données (clé usb, portable…). Sur le sol de l'Oncle Sam, il en est tout autre. La loi ***Hitech Act*** *(section 13402) impose l'affichage public de toutes fuites d'informations concernant plus de 500 patients dans le même établissement.*

En 1 an, la plus grosse fuite de données médicales aux USA aura visé l'Anthem, Inc. Affiliated Covered Entity. Nous sommons alors en mars 2015. 78,8 millions de dossiers suite à un « ***Hacking/IT Incident Network Server*** *» comme le référence le Ministère américain de la Santé (****HHS****). Depuis le 1er janvier 2016, 103 établissements de santé (Hôpitaux, centres de soin…) ont été touchés par une perte, un vol, un piratage. Dernier cas en date, 2.213.597 de données de patients piratés au 21st Century Oncology de Floride. Ici aussi, le HHS (U.S. Department of Health and Human Services) parle de «* ***Hacking/IT Incident Network Server****« . L'attaque date du 4 avril 2016.*

Depuis le 1er janvier 2016, 3.605.511 dossiers de patients américains ont volés, piratés ou perdus. Et en France ?

Article 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

Source : *ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ*

Après 3 semaines d'insistance de ZATAZ, la CNIL fait corriger une fuite de données sur le site du PS en quelque heures

Après 3 semaines d'insistance de ZATAZ, la CNIL fait corriger une fuite de données sur le site du PS en quelque heures

---

Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

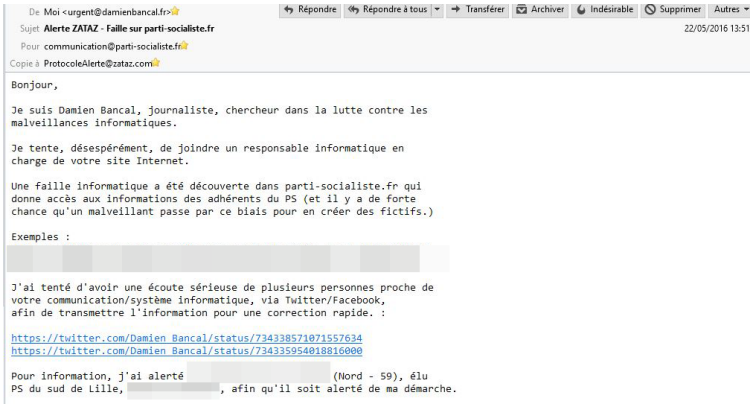
Des fuites de données, j'en croise des dizaines par mois, des centaines par années. Depuis la création de mon blog, voilà plus de trente ans (sur disquette, puis papier) et bientôt 20 ans sur le web, ZATAZ a pu aider plus de 60.000 entreprises, associations, particuliers à se protéger des malveillants du web. Bref, permettre de corriger une fuite de données, une faille, un problème de piratage via le protocole d'alerte ZATAZ.

Dans 99,9% des cas, cela se passe bien, voire très très bien. Pour les cas étatiques, par exemple, l'ANSSI me répond dans la minute, même un dimanche, à 3h du matin. La CNIL ne met pas plus de temps. Seulement, il y a ce 0,1 % de … J'ai un mot en tête, mais n'étant pas grossier de nature, je vous laisse l'imaginer.

Allô ! le Parti Socialiste ? vous avez une fuite de données !

Il y a trois semaines, je constatais une étonnante fuite de données visant un sous domaine du site Internet du Parti Socialiste. Je passerai le côté technique de la chose. Il suffisait de cliquer sur un lien particulièrement formulé vers le sous dossier « Archive » pour que s'ouvre un espace d'administration du portail politique du PS.

Le « oueb » de ce groupe politique fait parti du 0,1 % de cette froideur intellectuelle et de « je-m'en-foutisme » qui pourraient coûter très chers si un interlocuteur moins impliqué que moi avait eu en main l'accès à cette fuite de données. Car fuite de données il y avait. Il était possible d'accéder aux noms, prénoms, adresses physiques, mails des adhérents, montant des cotisations, code dossier, département … de l'espace adhésion (en attente de traitement, transmise, non finalisée et effective).



De Moi <urgent@damienbancal.fr>
Sujet **Alerte ZATAZ - Faille sur parti-socialiste.fr**
Pour communication@parti-socialiste.fr
Copie à ProtocoleAlerte@zataz.com

Répondre | Répondre à tous | Transférer | Archiver | Indésirable | Supprimer | Autres
22/05/2016 13:51

Bonjour,

Je suis Damien Bancal, journaliste, chercheur dans la lutte contre les malveillances informatiques.

Je tente, désespérément, de joindre un responsable informatique en charge de votre site Internet.

Une faille informatique a été découverte dans parti-socialiste.fr qui donne accès aux informations des adhérents du PS (et il y a de forte chance qu'un malveillant passe par ce biais pour en créer des fictifs.)

Exemples :

J'ai tenté d'avoir une écoute sérieuse de plusieurs personnes proche de votre communication/système informatique, via Twitter/Facebook, afin de transmettre l'information pour une correction rapide. :

https://twitter.com/Damien_Bancal/status/734338571071557634
https://twitter.com/Damien_Bancal/status/734335954018816000

Pour information, j'ai alerté [redacted] (Nord - 59), élu PS du sud de Lille, [redacted], afin qu'il soit alerté de ma démarche.

Bref, après deux mails au service presse (sans réponse) ; deux mails aux DSI BS et JW (sans réponse) ; plusieurs Tweets dont une discussion hallucinante avec l'un des DSI que je tentais de contacter, autant dire qu'au bout de trois semaines, j'ai beau faire cela bénévolement, la moutarde commençait à me monter au nez, surtout après la lecture de plusieurs articles indiquant que d'étonnantes adhésions au PS étaient apparues dans plusieurs circonscriptions (Metz, …). Je me suis résolu à contacter des élus du PS officiant dans ma région, ainsi que la CNIL. Autant dire qu'avec la prestigieuse dame, cela n'aura pas pris trois semaines. Deux heures après mon alerte à la Commission Informatique et des Libertés, l'étonnant accès disparaissait du web… [Lire la suite]

Article de Damien Bancal

Réagissez à cet article

Source : *ZATAZ La CNIL fait corriger une fuite de données sur le site du PS – ZATAZ*

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?

Arrêté en Belgique le 18 mars 2016 suite aux attentats de Paris du 13 novembre 2015, Monsieur Salah Abdeslam a été mis en examen notamment pour assassinats et tentatives d'assassinats en bande organisée en relation avec une entreprise terroriste, et placé en détention provisoire le 27 avril à la maison d'arrêt de Fleury Mérogis, dans l'attente de son jugement.

Il est aujourd'hui placé en isolement total dans une cellule de 9m2, et deux caméras le filment 24h/24. Cette mesure, tout-à-fait exceptionnelle, est justifiée, selon le Ministre de la Justice français, "conformément aux exigences la Convention Européenne de Sauvegarde des Droits de l'Homme et du droit français de la protection des données personnelles".
La loi française prévoit un régime dérogatoire s'agissant de la procédure pénale en matière de terrorisme, mais aucune disposition n'envisage spécifiquement la mise en place d'un dispositif de surveillance continue de la cellule d'un détenu. La Cour Suprême française (Cour de Cassation) a retenu à une reprise, en matière de criminalité organisée, la validité de la sonorisation permanente d'une cellule, sur autorisation du juge d'instruction.
Un arrêté français du 23 décembre 2014 autorise le contrôle sous vidéoprotection d'une cellule de protection d'urgence, mais ce texte ne vise que les détenus "dont l'état apparaît incompatible avec leur placement ou leur maintien en cellule ordinaire en raison d'un risque de passage à l'acte suicidaire imminent ou lors d'une crise aigüe" et alors la durée d'enregistrement ne peut dépasser 24 heures consécutives. C'est dans l'une de ces cellules de protection d'urgence pour les détenus suicidaires que monsieur Salah Abdeslam est actuellement détenu. L'arrêté ne serait donc applicable que s'il était démontré un risque imminent de passage à l'acte suicidaire, alors que Monsieur Salah Abdeslam est isolé, ses visites étant très limitées, et complètement isolé des autres détenus à chaque promenade. Il dispose en outre d'un pyjama en papier, sa cellule vide faisant l'objet d'une surveillance accrue par des rondes renforcées toutes les 3 heures. Monsieur Salah Abdeslam lui-même est encadré par une équipe de surveillants et médecins spécialisés dans les personnes dangereuses.
La Cour Européenne des Droits de l'Homme a permis aux détenus de bénéficier d'une véritable protection de leurs droits, en s'appuyant notamment sur l'article 3 de la convention, relatif aux traitements inhumains et dégradants. Les états membres doivent en effet s'assurer que la détention est compatible avec le respect de la dignité humaine et à veiller à ce que la santé et le bien-être du prisonnier soient assurés de manière adéquate. La Cour a déjà tenu compte, dans une affaire d'isolement carcéral et dans un contexte de la lutte contre le terrorisme, de la personnalité du détenu et de sa dangerosité hors norme, pour justifier de la mise en place de telles mesures (CEDH Grande Chambre, 4 juillet 2006, Ramirez Sanchez c/ France).
En matière de vidéosurveillance continue, la Cour Européenne a déjà été saisie de cette question, mais n'y a pas répondu, estimant que le requérant n'avait pas épuisé toutes les voies de recours internes dont il bénéficiait pour contester l'application de la mesure de sa vidéosurveillance (CEDH, Riina c/ Italie, 11 mars 2014). Le requérant, condamné à la réclusion à perpétuité pour association de malfaiteurs de type mafieux et de multiples assassinats se plaignait d'une vidéosurveillance constante dans sa cellule, y compris dans les toilettes.
Conscient de ce vide juridique, le Ministère de la Justice français a saisi l'autorité française de contrôle et de protection des données personnelles (CNIL), en charge notamment des questions liées la conservation des enregistrements et des mesures de vidéoprotection, d'un projet d'arrêté sur la vidéosurveillance en prison. Son avis sera rendu public dans les prochains jours.
En cas d'avis défavorable de la CNIL, l'avocat de Salah Abdeslam serait en droit de contester la mesure et de réclamer, outre une réduction de la mesure de vidéoprotection, une indemnisation financière devant le directeur de la prison, et en cas de rejet, de saisir le juge administratif français d'un recours. A charge pour l'avocat d'inscrire cette procédure de contestation dans une stratégie de défense plus générale… [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Source : *Pourquoi la vidéosurveillance 24h/24 de Salah Abdeslam pose question légalement*

RGPG Règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès

RGPD Règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès

---

Philippe Carrère, directeur de la protection des données et de l'identité, Europe du Sud chez Gemalto revient sur le nouveau règlement européen sur la protection des données personnelles et ce qu'il implique pour les entreprises en termes de stratégie de sécurité et de relation client.

L'adoption récente du règlement européen sur la protection des données personnelles constitue un tournant pour les entreprises implantées dans l'Union Européenne. En effet, il exige des gestionnaires d'infrastructures et des fournisseurs de services numériques – tels qu'Amazon ou Google – de faire part d'éventuels vols de données et de mettre en place des mesures de sécurité adéquates. Les chefs d'entreprises devraient y voir là un avertissement et commencer dès à présent à évaluer leurs politiques de sécurité, avant que la proposition de loi ne soit approuvée par le Parlement et le Conseil européen.
Où en sont les entreprises européennes en termes de sécurité des données et quelles mesures doivent-elles prendre afin d'être conformes ? A l'heure actuelle, les pare-feu, les antivirus, le filtrage de contenu et la détection des menaces sont les principaux outils utilisés pour se prémunir des vols de données. Ces mesures sont, cependant, insuffisantes, les hackers pouvant franchir aisément ce premier périmètre de sécurité. Dès lors, l'adresse IP des entreprises ou encore les informations de leurs clients peuvent être compromises, comme ce fut le cas avec Volkswagen et la conception de sa Passat.
D'après le Breach Level Index réalisé pour l'année 2015 par Gemalto, plus de 707,5 millions de dossiers clients ont été volés ou perdus à la suite de 1 673 cyberattaques menées de par le monde. Un chiffre qui devrait faire l'effet d'un véritable électrochoc pour les responsables informatiques, d'autant que, fait encore plus inquiétant, 4 % des infractions ont impliqué des données sécurisées (chiffrées partiellement ou en totalité).
Les clients confient des données confidentielles, et ils doivent donc être assurés et convaincus de leur sécurité. Si le lien de confiance avec le client vient à être brisé, il peut être très difficile pour les entreprises de le renouer.
Une de nos récentes études a révélé que plus de la moitié des individus interrogés (57 %) ne traiterait jamais, ou très peu probablement, avec une société ayant perdu des données personnelles suite à une cyberattaque.

Pourquoi ce règlement apparaît aujourd'hui comme une nécessité ?
La sécurité a toujours été un sujet d'actualité, mais suite aux récentes attaques, comme celle de Talk Talk, et le fait que de plus en plus de données personnelles sont collectées en ligne, assurer leur sécurité et maintenir une relation de confiance avec les clients n'a jamais été aussi primordial. A l'heure actuelle, les entreprises européennes ne sont pas tenues de signaler les brèches de données dont elles peuvent faire l'objet, et, de fait, grand nombre d'entre elles ne le font pas. Une fois la nouvelle réglementation en vigueur, elles seront dans l'obligation de révéler ces violations, sous peine de se voir infliger une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. C'est pourquoi elles doivent dès à présent opérer un changement de stratégie.
Cependant, il ne s'agit pas là d'un fait nouveau. Cette pratique est déjà en place depuis plusieurs années aux Etats-Unis. C'est pourquoi nous entendons davantage parler des cyberattaques ayant lieu outre-Atlantique que celles se produisant près de chez nous.

Quels sont les principaux enseignements à en tirer ?
Au lieu de se concentrer uniquement sur la protection du périmètre de sécurité, les entreprises devraient plutôt adopter une approche segmentée, protégeant les données à tous les niveaux et barrant le passage aux hackers qui auraient franchi le 1er palier de défense. Cela signifie également que la priorité doit porter sur les données elles-mêmes et sur le fait qu'elles ne puissent être consultées ou utilisées par des personnes non autorisées. Protéger les données par des solutions de chiffrement de bout en bout, d'authentification et des contrôles d'accès permet d'ajouter un niveau de sécurité supplémentaire. En mettant en place des outils de chiffrement, les données subtilisées n'ont plus aucune valeur pour toute personne non autorisée. L'accès peut être sécurisé en utilisant des clés permettant aux personnes habilitées de consulter les informations. Ainsi, en cas d'attaque, les entreprises sont certaines de garantir la sécurité des données de leurs clients.

Informer les clients
Une fois ces mesures sécuritaires mises en place, il est important d'en informer les clients et de les rassurer quant à la pertinence des processus instaurés pour protéger leurs données. Si les entreprises peuvent démontrer qu'elles sont prêtes à se dépasser et à mettre toute leur énergie dans cette démarche, elles seront perçues comme innovantes et dignes de confiance.
La sécurité est un effort mutuel. S'il est important d'informer les clients sur le travail qui est fait pour assurer leur sécurité, il est tout aussi primordial qu'ils sachent comment se protéger eux-mêmes. De plus, s'adresser à un utilisateur averti permettra de lui proposer un meilleur service client.
L'adoption du nouveau règlement européen sur la protection des données donne aux entreprises la possibilité de prendre les devants et montrer dès à présent à leurs clients qu'elles prennent ce sujet très au sérieux. Elles ne doivent pas seulement se soucier d'être conformes ou pas, mais comprendre qu'il s'agit là d'une nécessité essentielle à leur réussite. Les utilisateurs sont de plus en plus conscients qu'ils confient des données sensibles aux entreprises, leur demandant, de fait, d'en être responsables. La montée en puissance de cette prise de conscience doit aller de pair avec un niveau d'exigence plus élevé vis-à-vis des structures hébergeant ces informations. Ne pas prendre ce sujet au sérieux pourrait non seulement être préjudiciable en cas d'attaque, mais également nuire à la confiance instaurée avec les clients. Perdre ce lien les incitera à se tourner vers des concurrents jugés plus fiables… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès | Solutions Numériques*

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

CNIL. Commission Nationale de l'Informatique et des Libertés	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*

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 »*

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