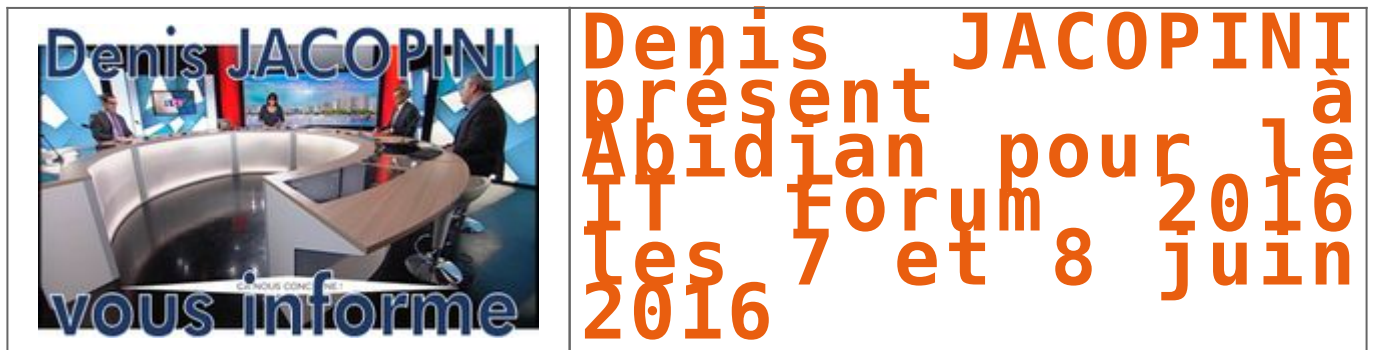


Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016



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



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 sommes 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.



[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



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/73433954018816000

Pour information, j'ai alerté (Nord - 59), élu PS du sud de Lille, , 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



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.



[Contactez-nous](#)

Réagissez à cet article

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

La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique

CNIL Délibération de la formation restreinte n° 2016-108 du 21 avril 2016 prononçant un avertissement à l'encontre de la société RICARD La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, Mme Marie-Hélène MITJAVILE, Mme Dominique CASTERA, M. Maurice RONAI, membres ; Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ; Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ; Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ; Vu la décision n° 2015-200C du 8 juillet 2015 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous les traitements relatifs au site RICARD.COM ; Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 8 janvier 2016 ; Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ; Vu la demande de huis clos présentée par la société RICARD le 25 janvier 2016 à laquelle il a été fait droit par courrier du 4 février 2016 ; Vu les observations écrites versées par la société RICARD le 19 février 2016 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;	La CNIL inflige une sanction à Ricard pour défaut de sécurité
---	--

La CNIL vient de publier un avertissement public contre Ricard pour défaut de sécurisation des données d'un programme de fidélité accessible sur le web.



Délibération de la formation restreinte n° 2016-108 du 21 avril 2016 prononçant un avertissement à l'encontre de la société RICARD

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDIN, Vice-président, Mme Marie-Hélène MITJAVILLE, Mme Dominique CASTERA, M. Maurice RONAI, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2015-200C du 8 juillet 2015 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous les traitements relatifs au site RICARD.COM ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 8 janvier 2016 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société RICARD le 12 janvier 2016 ;

Vu la demande de huis clos présentée par la société RICARD le 25 janvier 2016 à laquelle il a été fait droit par courrier du 4 février 2016 ;

Vu les observations écrites versées par la société RICARD le 19 février 2016 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Voilà une publicité dont Ricard se serait bien passé mais la sanction est cependant bien légère. La CNIL vient en effet de sanctionner le distributeur de produits alcoolisés pour un programme de fidélité présenté sur son site web. Les données personnelles des membres de ce programme n'étaient en effet pas protégées. L'autorité administrative indépendante, constatant l'absence de préjudice réel et la correction du problème, n'a cependant pas sanctionné très durement l'entreprise puisqu'elle lui a juste infligé un avertissement public par une décision du 21 avril 2016 publiée le 24 mai.

Concrètement, les données personnelles (noms, prénoms, dates de naissance, moyens de paiements, achats opérés, adresses électroniques, téléphones...) étaient stockées dans un répertoire du site web qui n'était ni bloqué en accès (par un .htaccess par exemple) ni crypté. La seule précaution prise était une demande de désindexation du répertoire dans les moteurs de recherche via une instruction dans le robot.txt. Donc, une simple lecture durobot.txt, par nature en clair, permettait de savoir où chercher des informations intéressantes.

Incompétence du prestataire, indifférence du responsable de traitement

Après un premier contrôle opéré le 8 juillet 2015, la CNIL prévient Ricard du problème. La société déclare avoir effectué le nécessaire en le commandant à son prestataire, information confirmée par un courrier du 23 juillet. Or, le 27 novembre 2015, un nouveau contrôle aboutit au constat que, certes, l'affichage du contenu du répertoire indiqué dans lerobot.txt n'est plus possible mais l'accès en lecture aux URL directes des fichiers l'est toujours ! Un nouveau procès-verbal d'infraction lui est donc adressé le 4 décembre 2015, notification à l'origine de la procédure dont nous parlons ici. Le site web a finalement été refondu pour être à l'état de l'art en matière de sécurité.

Cette affaire est l'occasion de plusieurs rappels intéressants. Tout d'abord, pour la CNIL, le seul et unique responsable est et demeure l'entreprise qui ordonne la création et maîtrise le traitement de données. Cette entreprise ne peut en aucun cas se défaire sur un prestataire. C'est au commanditaire de bien vérifier la mise en place des mesures obligatoires. Mais, et c'est induit, le commanditaire, responsable du traitement, doit effectivement commander et vérifier la mise en place des telles mesures.

Une mise en cause du prestataire délicate

La délibération de la CNIL ne mentionne pas le sous-traitant en cause. Une porte-parole de la CNIL précise : « pour l'instant, le seul responsable pour nous est Ricard en tant que responsable du traitement même si, avec le nouveau Règlement Européen, la place du prestataire va évoluer. » Le groupe Pernod-Ricard, sollicité par la rédaction, n'a pas encore officialisé une réaction ni précisé quel était le prestataire en cause.

Cela dit, dans l'absolu, le prestataire pourrait être poursuivi civilement par Ricard. Le producteur de pastis pourrait lui demander une indemnisation pour le préjudice subi de son fait, notamment le préjudice d'image.

Mais encore faudrait-il que la faute puisse être caractérisée et prouvée. En effet, les attentes en matière de sécurité doivent être spécifiées contractuellement pour qu'un manquement soit caractérisé. Et les instructions du commanditaire, Ricard en l'occurrence, ne doivent pas être contraaires directement ou indirectement aux bonnes pratiques. En général, ce genre d'affaires se règle discrètement dans les bureaux des entreprises concernées et il est peu probable que le résultat de ces palabres ne soit un jour connu.

MISE À JOUR : COMMUNIQUÉ DE RICARD

En réponse à notre sollicitation, Ricard nous a fait parvenir un communiqué laconique, sans citer le prestataire mis en cause, mais insistant sur les limites du manquement relevé par la CNIL. « Suite à la délibération de la CNIL du 21 avril 2016 prononçant un avertissement à l'encontre de la société Ricard pour son site internet Ricard.com, la société Ricard prend acte de cette décision et précise, comme le rappelle la CNIL, que la faille de sécurité identifiée a été corrigée sur le site existant. La société Ricard entend préciser que les données étaient exclues d'une indexation sur Internet et n'ont donc jamais été accessibles par des moteurs de recherche. La société Ricard confirme en outre avoir développé un nouveau site Ricard.com qui sera mis en ligne début juin et qui répond également aux normes de sécurité ».

Article de Bertrand Lemaire



Réagissez à cet article

Source : *La CNIL inflige une sanction à Ricard pour défaut de sécurité – Le Monde Informatique*

Deux applications accusées d'espionner les coureurs



Deux applications accusées d'espionner les coureurs

Les applications Runkeeper et Tinder viennent d'être dénoncées par le conseil des consommateurs norvégien. En effet, elles exploiteraient illégalement les données des utilisateurs.



Si vous ne le savez pas encore, Runkeeper est une application qui permet de mesurer ses performances sportives. Si on parle d'elle aujourd'hui, ce n'est pas vraiment pour les fonctionnalités qu'elles proposent, mais plutôt pour un sujet plus serré. En effet, cette application qui est la possession de la société FitnessKeeper violerait les règles de confidentialité des données personnelles. D'après le NCC (conseil des consommateurs norvégien), afin de pouvoir évaluer l'état de l'utilisateur, elle doit d'abord accéder à des fonctionnalités stratégiques telles que la géolocalisation.

Et le comble dans tout cela, c'est le fait que les données de l'utilisateur ayant été collectées seraient ensuite utilisées pour des finalités commerciales. En effet, elles seraient revendues à des entreprises de publicité et seraient même sauvegardées même après la suppression du compte. En tout cas, c'est ce qu'avance un rapport qui date du 10 mai. Interrogé sur cette question, le fondateur de Runkeeper a indiqué que le problème vient d'un bug. « Nous sommes en train de sortir une nouvelle version de notre application qui élimine ce bug... Nous prenons au sérieux la confidentialité des données des utilisateurs... », a-t-il indiqué. Par ailleurs, outre l'application Runkeeper, le NCC pointe aussi du doigt l'application Tinder, laquelle est une application pour les fans de rencontre amoureuse. Elle, aussi, conserverait les données des utilisateurs, notamment, les photos et les conversations... [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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Runkeeper et Tinder : les deux applications accusées d'espionner les coureurs – MeilleurActu*

Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint

	Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques
--	---

Impossible d'échapper aux mécanismes de recommandations sur Internet. Tous les sites internet, marchands ou réseaux sociaux, utilisent désormais ces fameuses recommandations censées influencer nos comportements d'achats. Basées sur de l'intelligence artificielle de plus en plus puissante, les recommandations se font plus pertinentes. Dans l'avenir elles pourront tirer profit d'une connaissance précise de notre personnalité comme le montre une étude réalisée à partir de l'analyse des « likes » de Facebook.



J'aime

Toute action sur Internet se transforme en données. On s'inquiète à juste titre de l'usage qui est fait de nos données personnelles (voir mon billet sur Safe Harbor). L'annonce par Facebook de « Search FYI » devrait encore attirer notre attention sur la protection de notre vie privée. Avec Search FYI, Facebook peut rechercher des informations dans tous les messages publics publiés par ses membres. Avec le développement de l'intelligence artificielle et l'utilisation du machine learning la valeur des données monte en flèche. Le mot « donnée » est souvent sous-estimé. On comprend bien qu'une photo et un texte postés sur un réseau social sont des données mais on oublie que le simple fait de cliquer sur un « like » devient une donnée aussi importante voire plus. Toute action sur internet laisse une trace numérique qui pourra être exploitée. C'est la base même du marketing digitale qui utilise ces traces numériques laissées sur le parcours client pour mieux connaître le consommateur et augmenter l'expérience utilisateur. C'est du donnant donnant : mieux nous sommes connus, mieux nous sommes servis. C'est l'évolution naturelle liée à la transformation numérique.

En analysant les « Likes », Facebook en sait plus sur notre personnalité que nos proches. La personnalité est un concept complexe qui semble difficilement mesurable. Cela touche à des sentiments, des émotions, des valeurs qui nous façonnent et qui nous rendent uniques. On pourrait donc imaginer, voire espérer, que les ordinateurs puissent se montrer impuissants à « quantifier » ce qui nous définit en tant qu'être humain. Pourtant une étude menée par des chercheurs des universités de Cambridge et de Stanford, publiée en janvier 2015, a montré que l'Intelligence Artificielle a le potentiel de mieux nous connaître que nos proches. Cette étude visait à comparer la précision d'un jugement sur la personnalité réalisé par un ordinateur et des êtres humains. Les chercheurs ont demandé à 86.200 volontaires de leur donner accès à leurs « Likes » sur Facebook et de répondre à un questionnaire de 100 questions sur leur personnalité. Ces données ont été modélisées et le résultat est assez étonnant. On apprend que :

Avec l'analyse de 10 likes, Facebook en sait plus sur nous que nos collègues

Avec 70 likes Facebook en sait plus que nos amis

Avec 150 likes Facebook en sait plus que notre famille

Avec 300 likes Facebook en sait plus que notre conjoint

Quand on sait qu'en moyenne un utilisateur Facebook a 227 Likes, on se dit que nous n'avons plus grand choses à cacher.

Partager des émotions comme on partage des photos ou des vidéos. C'est la prochaine étape qu'imagine Mark Zuckerberg dans le futur. Durant une session de questions réponses sur son profile Facebook, le patron de Facebook a expliqué qu'il pensait que nous aurions à l'avenir la possibilité de partager nos expériences émotionnelles rien que par le seul fait d'y penser. La télépathie appliquée aux réseaux sociaux ? En matière d'Intelligence artificielle il devient difficile de faire la différence entre science-fiction et prévision. Quoiqu'il en soit Gartner a rappelé que c'étaient les algorithmes qui donnaient leur valeur aux données. Le progrès de ces algorithmes et leur complexité justifient qu'on s'intéresse à la protection de notre vie privée. Ils deviennent incontournables dans notre vie moderne, il faut en être conscient... [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.



[Contactez-nous](#)

Réagissez à cet article

Source : Avec l'intelligence artificielle, Facebook en sait autant sur vous que votre conjoint. – Entreprises Numériques

Pourquoi la vidéosurveillance de Salah Abdeslam pose question légalement ?



Arrêté en Belgique le 10 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 vidéosurveillance 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 aiguë" 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'arresté 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 cybersécurité et en protection des
données personnelles.

- Expertises techniques (virus, worms, parasites,
malwares, attaques Internet...) et judiciaires
(investigation téléphonique, diques dark, e-mail,
contrefaçon, détournement de clientèle...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybersécurité ;
- Formateur de C.I.L. (Correspondants Informatique
et Libération) ;
- Accompagnement à la mise en conformité CNIL
de votre établissement.



Contactez nous

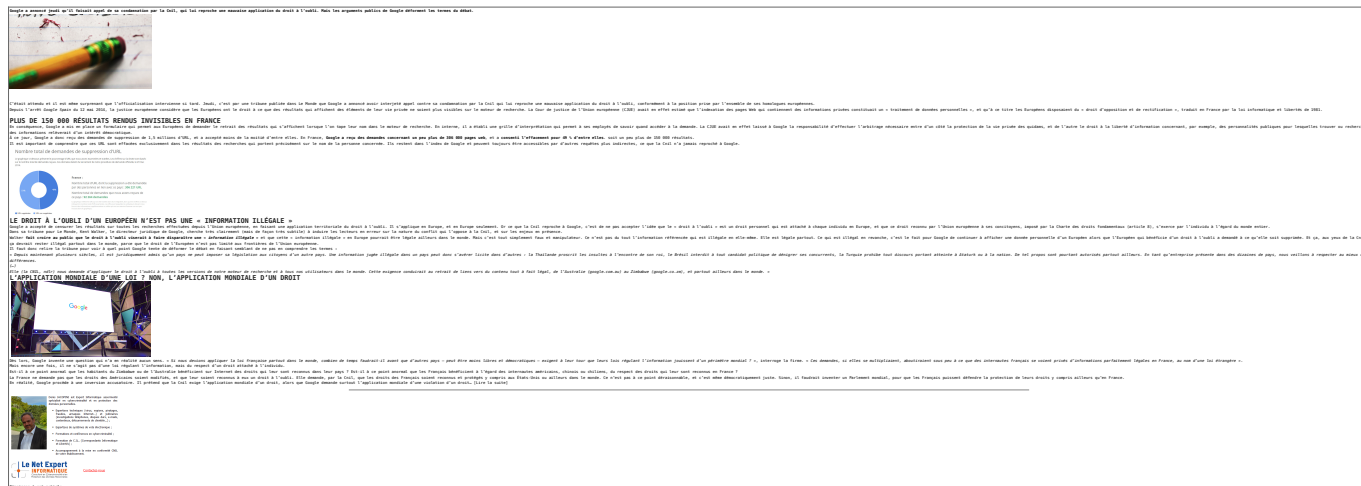
Régistrez à cet article

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

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil



Google fait
semblant de ne
rien comprendre
à ce qu'exige la
Cnil



Et si la reconnaissance faciale de Facebook était excessive ?



Depuis 2010, Facebook propose à ses utilisateurs un système de reconnaissance faciale qui permet de gagner du temps dans le « taguage » des personnes qui sont sur les photos. Sous couvert d'une nouvelle fonctionnalité, c'est un véritable dispositif biométrique qui a été mis en œuvre car il permet d'identification d'un individu à partir d'une simple photographie de son visage.

En Californie, trois utilisateurs ont reproché au réseau social n°1 d'avoir « secrètement et sans leur consentement » collecté des « données biométriques dérivées de leur visage ». Ces plaintes ont été jugées recevables par le juge James Donato qui « accepte comme vraies les allégations des plaignants » et juge « plausible » leur demande.

Au sein de l'Union européenne, le danger a rapidement été perçu s'agissant du système de reconnaissance faciale de Facebook qui l'a suspendu en 2012. Mais aux Etats-Unis, bien moins vigilants, cette fonctionnalité a perduré et il apparaît bienvenu que la Justice y réagisse enfin. Facebook a constitué des profils qui répertorient les caractéristiques du visage de ses utilisateurs, leur cercle d'amis, leurs goûts, leurs sorties, etc. Avec plus de 3 milliards d'internautes dans le monde, cela revient à ce qu'environ 28% de la population ait un double virtuel rien que sur Facebook.

Facebook is watching you : Reconnaissance faciale, intelligence artificielle et atteinte aux libertés

Eu égard à leur grand potentiel discriminatoire, les données biométriques sont strictement encadrées par la loi du 6 janvier 1978 puisque d'après son article 25, une autorisation préalable de la Commission nationale de l'informatique et des libertés est indispensable pour mettre en œuvre des « traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes ». Cela regroupe l'ensemble des techniques informatiques qui permettent d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les conditions générales d'utilisation de Facebook ne sont pas donc pas conformes à la législation française sur les données personnelles, notamment s'agissant de la condition de consentement préalable, spécifique et informé au traitement des multiples données à caractère personnel collectées. Mais le géant de l'internet ne répond qu'à l'autorégulation. Par opposition à la réglementation étatique, la régulation n'entend prendre en compte que la norme sociale, c'est-à-dire l'état des comportements à un moment donné. Si la norme sociale évolue, alors les pratiques de Facebook s'adapteront.

Vers une remise en cause mondialisée des abus de Facebook ?

L'affaire pendante devant les Tribunaux met en lumière le manque de réactivité des américains face aux agissements de Facebook. C'est seulement au bout de 5 années que la Justice s'empare de la question des données biométriques à l'initiative de simples utilisateurs, alors même qu'une action de groupe à l'américaine d'envergure aurait pu être engagée pour mettre sur le devant de la scène les abus de Facebook.

Néanmoins, « mieux vaut tard que jamais » et l'avenir d'une décision répressive ouvre la porte vers de nouveaux horizons pour l'ensemble des utilisateurs. En effet, Facebook prend comme modèle pour toutes ses conditions générales d'utilisation à travers le monde la version américaine de « licencing ». Plus Facebook se verra obligé dans son pays natal à évoluer pour respecter les libertés individuelles des personnes inscrites, plus on s'éloignera du système tentaculaire imaginé par Mark Zuckerberg qui n'est pas sans rappeler celui imaginé par Georges Orwell dans son roman 1984.

Par Antoine CHERON, avocat associé, est docteur en droit de la propriété intellectuelle, avocat au barreau de PARIS et au barreau de BRUXELLES et chargé d'enseignement en Master de droit à l'Université de Assas (Paris II). Il est le fondateur du cabinet d'avocats ACBM... [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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Facebook is watching you : système biométrique efficace – Data Security Breach*

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

Denis JACOPINI  vous informe	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.

Informers 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]



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.



[Contactez-nous](#)

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