Conséquences innatendues des cyberattaques

Conséquences innatendues des cyberattaques

Les dégâts informatiques de premier jour ne constituent pas la seule conséquence d'une cyberattaque pour une entreprise. Il y a aussi la réduction en nombre des clients, déçus notamment du vol ou de la perte de leurs données. Certains peuvent même penser à poursuivre l'entreprise en justice. L'après est ainsi encore plus dure à gérer pour les dirigeants et les responsables informatiques.

Impact sur la confiance des consommateurs

La préparation d'une cyberattaque peut prendre plusieurs semaines, voire des mois. Par conséquent, leurs effets vont bien au-delà des « simples » dégâts informatiques. Une étude internationale réalisée par VansonBourne et publiée le 12 mai dernier le confirme, en insistant sur des atteintes sur la performance commerciale de la société victime. Elle révèle en effet que la confiance des consommateurs vis-à-vis de cette dernière s'amenuise après les attaques. Logique quand on sait que bon nombre de clients de TV5 Monde et Orange ont encore du mal à oublier les attaques respectives d'avril 2015 et de 2014 ayant entraîné une fuite de données. Cette étude avance même que 34% des Français voient leur loyauté envers une marque ayant laissé fuiter leurs données, diminuée. Les efforts de cybersécurité devront ainsi se trouver dans le plan de toute entreprise qui se veut être compétitive.
Les consommateurs sont également nombreux à perdre le désir d'acheter auprès d'une entreprise victime d'une attaque informatique. Plus de trois sur quatre ont même affirmé qu'ils iraient jusqu'à arrêter l'achat de produits ou services chez cette dernière, notamment si la vulnérabilité exploitée provient de l'erreur de l'équipe dirigeante. Pour une erreur humaine d'un subordonné, les clients sont plus compréhensifs. La publication de cette étude confirme par ailleurs que la sécurité des données figure depuis quelques années parmi les critères les plus considérés par les Français avant une décision d'acheter. Ce paramètre a été pris en compte par 61% des Français en 2015, contre 53% en 2014.

Risques de poursuite en justice

La perte de chiffre d'affaires est donc quasiment incontournable pour toute entreprise qui vient de faire l'objet d'une attaque informatique d'ampleur. Elle est toutefois moins grave par rapport à un autre risque, celui de la poursuite en justice. Cette étude a en effet permis de connaître que 50% des Français sont prêts à poursuivre en justice les entreprises attaquées pour négligence ou inattention apportée à la protection de leurs données personnelles. Target et Sony Picture en ont déjà payé le prix, trouvant même, parmi les auteurs de ces poursuites, leurs propres salariés. Face à ce risque, certaines entreprises envisagent de garder secrètes toutes les attaques atteignant leur système d'information. Serait-ce une bonne initiative de leur part ? La réponse est non. A l'heure d'Internet, la moindre information peut se trouver à la portée de tout le monde. Une éventuelle fuite pourrait ainsi écorner définitivement l'image d'une société choisissant une telle démarche. Au contraire, cette société devrait plutôt informer le plus rapidement ses clients, pour faire preuve de transparence. Cette démarche sera par ailleurs rendue obligatoire par le règlement européen sur la protection des données, un texte dont la mise en vigueur est prévue en mai 2018.

Article original de sekurigi.com complété par Denis JACOPINI

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les traces laissées par les cyberattaques – @Sekurigi

Privacy Shield : un « bouclier » troué à refuser !

	#Privacy Shield : un « bouclier » troué à refuser !

Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette décision, adoptée dans la plus grande précipitation, ne répond pas aux inquiétudes exprimées ces dernières semaines à tour de rôle par le groupe des CNILs européennes, le Parlement européen et différents gouvernements européens, ainsi que par les associations de défense des droits.

Le 6 octobre 2015 la Cour de justice de l'Union européenne avait annulé l'accord du « Safe Harbor » couvrant les transferts de données depuis 2000, estimant que celui-ci permettait une collecte massive des données et une surveillance généralisée sans offrir de voies de recours effectives aux États-Unis pour les individus concernés en Europe. Aujourd'hui, force est de constater que le Privacy Shield ne répond pas non plus aux exigences de la Cour de justice.
Sur les principes de respect de la vie privée qui incombent aux entreprises couvertes par le Privacy Shield, on peut se demander l'utilité même d'une telle décision dans la mesure où celle-ci ne se substituera pas aux clauses contractuelles types ni aux règles internes d'entreprises, moins contraignantes et actuellement en vigueur, mais qu'elle s'y ajoutera. Cela signifie que si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations qui lui incombent en matière de vie privée, elle pourra continuer à traiter des données avec les deux mécanismes internes cités plus hauts.
Mais le cœur de la décision se retrouve plutôt dans le chapitre sur l'accès aux données par les autorités publiques des États-Unis. Dans le texte, il n'est pas question de « surveillance de masse » mais plutôt de « collecte massive ». Or, si les États-Unis ne considèrent pas la collecte de masse comme de la surveillance, l'Union européenne, elle, par l'intermédiaire de sa Cour de justice, a tranché sur cette question en considérant, dans l'affaire C-362/14 Schrems c. Data Protection Commissioner, que la collecte massive effectuée par l'administration des États-Unis était de la surveillance de masse, contraire à la Charte des droits fondamentaux de l'Union européenne. Cette décision avait mené à l'invalidation du « Safe Harbor », et tout porte à croire que les voeux pieux et les faibles garanties d'amélioration exprimées par le gouvernement américain ne suffiront pas à rendre la décision du Privacy Shield adéquate avec la jurisprudence européenne.
Il en va de même sur la question des possibilités de recours. L'une des exigences de la CJUE, des CNIL européennes, du contrôleur des données personnelles et de la société civile était que toute personne concernée par un traitement de données avec cet État tiers puisse avoir la possibilité de déposer une plainte et de contester un traitement ou une surveillance illégale. Pour pallier cette sérieuse lacune du Safe Harbor, un mécanisme de médiateur (« #Ombudsperson ») a été instauré. L'initiative aurait été bonne si ce médiateur était réellement indépendant. Mais d'une part il est nommé par le Secrétaire d'État, d'autre part les requérants ne peuvent s'adresser directement à lui et devront passer par deux strates d'autorités, nationale puis européenne. L'Ombudsperson pourra simplement répondre à la personne plaignante qu'il a procédé aux vérifications, et pourra veiller à ce qu'une surveillance injustifiée cesse, mais le plaignant n'aura pas de regard sur la réalité de la surveillance. Cette procédure ressemble à celle mise en place en France par la loi Renseignement avec la #CNCTR et, pour les mêmes raisons, ne présente pas suffisamment de garanties de recours pour les citoyens.
Le projet de Privacy Shield, préparé et imposé dans la précipitation par la Commission européenne et le département du Commerce américain, ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. Les gouvernements européens et les autorités de protection des données doivent donc absolument refuser cet accord, et travailler à une réglementation qui protège réellement les droits fondamentaux. Les nécessités d'accord juridique pour les entreprises ayant fait de l'exploitation des données personnelles leur modèle économique ne peuvent servir de justification à une braderie sordide de la vie privée de dizaines de millions d'internautes européens.
Article original de La Quadrature du Net

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : un « bouclier » troué à refuser ! – Global Security Mag Online

---

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

Le Privacy Shield (« bouclier de protection des données personnelles »), un accord politique censé encadrer l'utilisation des données personnelles des citoyens Européens par les entreprises sur le sol américain, a été validé par les Etats membres, vendredi 8 juillet.

Pour la première fois, les Etats-Unis ont donné à l'Union européenne l'assurance écrite que l'accès des autorités aux données personnelles serait soumis à des limitations claires, des garde-fous et des mécanismes de contrôle, tout en écartant la surveillance de masse indiscriminée des données des Européens » s'est réjoui la commission dans un communiqué.

Le Privacy Shield est censé remplacer le Safe Harbor, un accord similaire qui a été invalidé par la Cour de justice de l'Union européenne (CJUE), qui a notamment cité le peu de cas que faisaient les agences de renseignement américaines des données personnelles des citoyens européens stockées sur le sol américain.
Les entreprises du numérique, placées dans une situation juridiquement inconfortable depuis l'annulation du Safe Harbor, ont salué cette étape supplémentaire sur le chemin de l'adoption définitive. « Même si les négociations n'ont pas été faciles, nous félicitons la commission et le ministère du commerce américain pour leur travail de restauration de la confiance dans les transferts des données entre l'UE et les Etats-Unis », a dit John Higgins, le directeur général de DigitalEurope, un lobby rassemblant notamment Google, Apple, Microsoft et IBM, qui dit aussi espérer que grâce au Privacy Shield « l'Europe puisse à nouveau se concentrer sur la manière dont les flux de données peuvent jouer un rôle dans la croissance économique ».

DE NOMBREUX OBSTACLES DEMEURENT

L'accord, entre la commission et les Etats-Unis, doit encore être validé par le collège des commissaires européens, avant son adoption définitive qui devrait intervenir le 12 juillet prochain, après des mois d'âpres négociations. Ce n'est pas la fin du débat autour de cet accord contesté.
L'accord n'a pas fait consensus auprès des Etats membres, les diplomates représentant plusieurs pays – l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters – se sont abstenus. Un moyen d'« exprimer leur méfiance vis-à-vis du texte » anticipait, jeudi lors d'une conférence, David Martinon, ambassadeur français pour la cyberdiplomatie et l'économie numérique, cité par le site Silicon.fr.
Par ailleurs, cet accord, sera très certainement contesté devant les tribunaux après son adoption. Max Schrems, l'Autrichien tombeur du prédécesseur du Privacy Shield, pourrait attaquer l'accord devant les juridictions européennes.
Dans le même ton, La Quadrature du Net, association française de défense des libertés numériques, a dénoncé un accord qui « ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. »
Article original de Martin Untinsinger

Réagissez à cet article

Original de l’article mis en page : Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

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

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

---

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

À très grands traits, selon la Cnil :

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

Peu de changements en vérité…

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

…Mais des changements piégeant à la marge

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

Une marge de manœuvre résiduelle

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

Article original de Didier Frochot

Réagissez à cet article

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

---

L'Etat français (ANSSI) va certifier les Cloud de

confiance

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

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

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

Deux niveaux : Cloud Secure et Cloud Secure +

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

Guillaume Poupard, directeur général de l'Anssi.

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

Cloud Secure + : les Américains out ?

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

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

---

Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique

Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique

Selon une information du quotidien De Morgen, le secrétaire d'Etat à la vie privée Philippe De Backer (Open Vld), estime que le gouvernement devrait être en mesure de transmettre des données relatives à la santé des citoyens belges au secteur pharmaceutique. « Nous pourrions demander de l'argent pour cela, à partir du moment où il y a un retour vers le patient », a expliqué De Backer.

Philippe De Backer présente sa note politique « Privacy » au Parlement. Dans celle-ci, il envisage un échange plus large des données personnelles des patients. Selon le secrétaire d'Etat, l'accès aux données et le traitement des données personnelles offrent d'importantes opportunités sociales et économiques. Les données publiques dans le domaine des soins de santé peuvent aboutir à des innovations intéressantes dans le secteur pharmaceutique, notamment en termes de prévention et vice-versa.

Compensation financière et contrôle du partage des données

En échange de ces informations privées, les patients pourraient recevoir une compensation financière. « Nous pourrions demander de l'argent pour cela, à partir du moment où il existe un juste retour pour le patient », a expliqué Philippe De Backer. Ce dernier évoque entre autres des prix moins élevés pour les médicaments des patients.

Par ailleurs, le secrétaire d'Etat souhaite également étendre la marge de manœuvre de la Commission de la vie privée. Celle-ci devrait déterminer quelles entreprises privées pourraient avoir accès aux données personnelles aux mains des pouvoirs publics. La Commission de la vie privée devrait également être en mesure d'infliger des amendes pouvant aller jusqu'à 4% du chiffre d'affaires pour les entreprises qui utilisent de façon inadéquate ces informations personnelles.

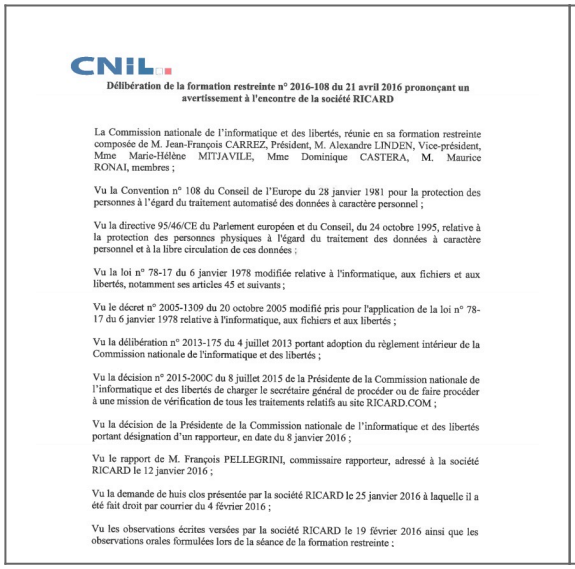
Philippe De Backer veut enfin que le patient ait davantage de contrôle sur la manière dont sont utilisées ses données. Dans ce sens, il évoque la création d'un passeport de confidentialité qui permettrait aux patients de savoir qui utilise leurs données personnelles.

Article original de Arnaud Lefebvre

Réagissez à cet article

Original de l'article mis en page : Le gouvernement pourrait partager vos données personnelles avec le secteur pharmaceutique – Express [FR]

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.

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 ;

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 du*robot.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 le*robot.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 défausser 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 contraires 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*

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*

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

---

Source : *Droit à l’oubli : Comment Google feint de ne rien comprendre à ce qu’exige la Cnil – Politique – Numerama*

Et si la reconnaissance faciale de Facebook était excessive ?

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 apparait 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 règlementation 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.

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

Contactez-nous

Réagissez à cet article

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