Comment protéger les données de vos enfants des pirates informatiques

Comment protéger les données de vos enfants des pirates informatiques

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Le piratage des jouets Vtech, puis la découverte d'une faille sur la plateforme en ligne du fabriquant Hello Kitty, posent aujourd'hui la question de la sécurité des données personnelles des enfants. Metronews vous livre ses conseils pour mieux protéger leurs informations.

Après l'annonce du piratage début novembre de VTech, le leader mondial des tablettes ludo-éducatives, c'est maintenant au tour d'Hello Kitty d'être accusée de mal sécuriser les données de ses utilisateurs. Pendant près d'un mois, les données personnelles de 3,3 millions de membres de la communauté en ligne du fabriquant japonais Hello Kitty (dont, évidement, beaucoup d'enfants) auraient été exposées en raison d'une faille de sécurité.

A quelques jour de Noël, ces deux affaires montrent clairement à quel point il est facile aujourd'hui pour les hackeurs de dérober des informations sensibles.Et aussi le danger qui peut en découler, comme le rappelle à metronews la Commission nationale de l'informatique et des libertés (CNIL) : « Nous constatons que certains secteurs industriels ajoutent une connectivité à leurs produits sans disposer historiquement d'une culture en sécurité informatique ».

► Vérifiez si votre mail est piraté
Il existe un moyen simple de savoir si votre adresse mail a été touchée. Pour cela, il faut se rendre sur le site haveibeenpwned.com. Entrez votre adresse mail, puis cliquez sur « pwned ? » pour lancer la recherche.
► Changez votre mot de passe
Par précaution, il est recommandé aux utilisateurs des services qui ont connu des intrusions de ce genre de changer leurs mots de passe. « Il doit être composé d'au moins 3 types de caractères différents parmi les quatre types de caractères existants : majuscules, minuscules, chiffres et caractères spéciaux ». Pour en savoir plus, rendez-vous sur le site de la CNIL.
► Ne communiquez que le minimum d'infos
Pour les enfants (et leurs parents), la CNIL recommande ainsi d'utiliser des pseudonymes sur les services en lignes, et de ne communiquer que le minimum d'informations. Par exemple, saisissez une date de naissance au 1er janvier si le système a besoin d'une indication de tranche d'âge.
► Veillez à bien lire les conditions d'utilisation
Outre les risques de sécurité révélés par la faille VTech, les parents doivent être vigilants concernant les possibilités de réutilisation des données collectées (profilage publicitaire) et s'assurer de la possibilité d'y accéder et de les supprimer.

Réagissez à cet article

Source : *Piratages VTech et Hello Kitty : comment protéger les données de vos enfants – metronews*

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

Panne électrique en Ukraine : le malware aurait été aidé par l’humain

---

 **Le mois dernier, une cyberattaque contre des fournisseurs d'énergie ukrainiens avait privé 80 000 clients d'électricité. D'après la signature du malware, l'attaque avait été imputée à un groupe de pirates ayant des liens avec la Russie. Mais, selon une nouvelle étude, le malware n'est pas directement à l'origine de la panne : les assaillants sont intervenus physiquement pour activer les disjoncteurs et provoquer la coupure de courant.**

Selon des informations publiées samedi par l'équipe du SANS Industrial Control Systems (ICS), une organisation spécialisée dans l'information et la formation des professionnels de la sécurité, le malware a bien servi aux pirates à s'introduire dans le réseau des fournisseurs d'électricité, mais ils sont ensuite intervenus sur les disjoncteurs pour couper l'alimentation. Depuis des années, les experts mettent en garde sur la vulnérabilité des systèmes de contrôle industriels. Les cyberattaques survenues le 23 décembre contre les installations ukrainiennes montrent que leurs craintes sont justifiées. Selon les experts du #SANS ICS, ces évènements sont aussi la preuve que de telles attaques sont planifiées et très coordonnées.
Depuis l'annexion de la Crimée par la Russie en 2014, les tensions entre la fédération et l'Ukraine restent fortes. « Pour masquer le piratage et l'intrusion dans les réseaux, les agresseurs sont intervenus physiquement sur la centrale électrique », a déclaré l'équipe du SANS ICS. « Les agresseurs ont également lancé en simultané une attaque DDoS par déni de service sur le réseau téléphonique afin de bloquer les appels des clients affectés par la panne », a encore déclaré l'organisation. Les attaques auraient visé les deux fournisseurs d'énergie Prykarpattyaoblenergo et Kyivoblenergo. Ce dernier a déclaré dans une mise à jour de service que 80 000 clients dépendant de 30 sous-stations avaient été déconnectés du réseau.

Des pannes provoquées par une action physique

Plusieurs entreprises de sécurité ont analysé le #malware Black Energy 3 et le #composant Killdisk utilisés pour les attaques. Jeudi dernier, l'entreprise de sécurité iSight Partners basée à Dallas a déclaré que ces logiciels malveillants avaient déjà été utilisés dans le passé par le #groupe de pirates Sandworm connu pour avoir de puissants intérêts russes. Mais, comme iSight, le SANS ICS pense que les pannes ne sont pas à mettre exclusivement sur le compte des malwares. « Autrement dit, de nouvelles preuves pourraient remettre en cause l'impact réel des composantes malveillantes impliquées dans l'attaque », a écrit Michael Assante, directeur du SANS ICS.
Le composant Killdisk écrase le Master Boot Record (MBR), premier secteur du disque dur chargé par le PC avant de monter le système d'exploitation, et empêche donc le PC de démarrer. Selon Symantec, Killdisk peut aussi écraser des fichiers en écrivant des données inutiles. Michael Assante avance que Killdisk n'était pas compatible avec le système SCADA de contrôle et d'acquisition de données utilisé par les deux opérateurs. Mais il a peut-être été utilisé pour effacer d'autres fichiers qui auraient permis la restauration des systèmes. « Il semble que les fournisseurs d'électricité ont rétabli leurs services en actionnant manuellement les disjoncteurs au bout de trois et six heures », a ajouté le directeur du SANS ICS. Selon lui, « il faudrait féliciter les opérateurs ukrainiens pour leur diligence et les efforts accomplis pour restaurer leurs services ».

Réagissez à cet article

Source : *Panne électrique en Ukraine : le malware n'est pas seul en cause – Le Monde Informatique*

Carte de paiement sans contact – Le client n’est pas toujours roi

Carte de paiement sans contact – Le client n’est pas toujours roi

---

Refuser les cartes bancaires équipées du paiement sans contact n’est pas toujours simple. Un client du Crédit agricole l’a appris à ses dépens.
En avril 2015, un adhérent de l’UFC-Que Choisir de Senlis saisit l’association locale de ses difficultés avec son agence du Crédit agricole de Rixheim (68). Celle-ci lui a adressé en renouvellement une carte bancaire Visa munie de la fonction paiement sans contact. Ayant lu dans Que Choisir que cette fonction n’était pas sans faille, ce consommateur demande à sa banque le remplacement de sa carte par une même carte Visa mais sans cette nouvelle fonction. Refus de son agence, puis de la direction régionale du Crédit agricole qui affirme que c’est impossible et lui propose en échange soit une carte Visa avec débit différé, soit un autre type de carte bancaire. Pas d’accord, le particulier fait part de ce blocage à l’association locale de l’UFC-Que Choisir de Senlis.

Client à la porte
L’intervention de cette dernière auprès de la banque n’aura pas plus de succès. Face à un tel refus, elle saisit la Cnil (Commission nationale de l’informatique et des libertés) au motif que le Crédit agricole viole une de ses recommandations qui impose aux banques d’offrir à leurs clients la possibilité de refuser la fonction paiement sans contact.
La Cnil rejette la plainte de l’association locale, déclarant ne pas pouvoir imposer aux banques un changement de carte à l’identique mais rappelle que le particulier a la possibilité de faire désactiver la fonction.
Fort de cette réponse, le consommateur demande à son agence cette désactivation.
Pour toute réponse, la banque a mis son client à la porte, le sommant de restituer tous ses moyens de paiement. La Cnil a été avertie d’un tel comportement.

Réagissez à cet article

Source : *Carte de paiement sans contact – Le Crédit agricole a la main leste – UFC Que Choisir*

FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données

	**#FIC 2016 les 25 et 26 janvier 2016 sur le thème de la sécurité des données**

Pendant longtemps, la sécurité des données se confondait avec celle de la sécurité des systèmes d'information. Or la décorrélation croissante entre le contenant (support physique ou applicatif) et le contenu en raison de l'émergence des technologies de virtualisation, du « cloud computing » et de nouveaux modèles économiques change aujourd'hui la donne. La donnée est devenue un « objet » à part entière qui s'appréhende indépendamment de son support.

Axe 1 : les données, carburant de la transformation numérique.

Les données sont omniprésentes et multiformes : on peut citer les données personnelles, sociales, médicales, bancaires, d'entreprises, de géolocalisation, de sécurité, de dossiers passagers (PNR) etc. Cette compartimentation en fonction des usages ou des secteurs d'activité a-t-elle cependant encore un sens ? Comment gérer l'information indépendamment des supports utilisés ? Au-delà de la métaphore, les données constituent-elles véritablement un « nouvel or noir » ?

Axe 2 : la maitrise des données, enjeu de souveraineté

Posséder une « industrie de la donnée » puissante est un atout essentiel dans la compétition mondiale et une composante importante de toute stratégie de puissance. Or l'Europe apparait de ce point de vue en net retrait par rapport aux Etats-Unis. Forte consommatrice de numérique, la faiblesse de son offre locale la conduit à exporter massivement ses données, principalement aux Etats-Unis. Comment passer d'une « Europe offerte » à une Europe « ouverte » ? Quelle est la situation des autres continents ? Peut-on parler de « géopolitique des données » ?

Axe 3 : les données, un capital menacé

Si les attaques en déni de service visent les infrastructures elles-mêmes, les données sont souvent l'objectif ultime des attaquants, qu'il s'agisse de cybercriminalité (vol d'information, crypto-locking…) ou d'espionnage. Quelles sont les dernières tendances observées ? Quels sont les modes opératoires des cybercriminels ? Comment calculer la valeur de ses données pour engager des poursuites ?

Axe 4 : droit et données

La donnée est une notion immatérielle qui soulève de nombreuses questions au plan juridique. Peut-on appliquer la notion de propriété à la donnée, notamment à la donnée personnelle ? Quel lien entre données et territoire ? Comment mettre en œuvre efficacement le droit à l'oubli aujourd'hui consacré dans certains pays ? Comment définir le vol de données au plan pénal ?

Axe 5 : quelles stratégies de sécurité des données pour l'entreprise ?

Pour les entreprises, la sécurité des données repose sur une approche globale impliquant : classification des données, évaluation des données, analyse de risques, définition et mise en œuvre d'une stratégie de sécurité. Le développement du cloud computing et l'externalisation croissante de l'IT soulèvent à cependant de nombreuses questions. Peut-on utiliser « en toute sécurité » un CRM ou un ERP dans le Cloud ? Quelles conséquences en termes de maîtrise des données ? Comment assurer les risques liés aux données ?

Axe 6 : quelles technologies pour sécuriser les données ?

Le responsable sécurité des systèmes d'information dispose aujourd'hui d'une vaste bibliothèque d'outils et de technologies lui permettant de sécuriser ses données, qu'il s'agisse d'outil de protection, de destruction sécurisée, de détection de fuites d'information ou d'investigation. La vitesse du progrès technologique et le « time to market » imposé par le marché aux éditeurs sont-elles compatibles avec les cycles d'adoption relativement lents des organisations ? Compte tenu de ce même « time to market », comment intégrer la sécurité de façon native (security by design) dans les applications à disposition des utilisateurs ?

Axe 7 : données et enjeux sectoriels

La transformation numérique et les données qui la nourrissent irriguent l'ensemble des secteurs économiques et des activités humaines. Les données sont ainsi au cœur de la « smart revolution » qui touche aussi bien l'individu dans sa vie quotidienne, la collectivité ou l'entreprise au travers des objets connectés et de « l'informatique omniprésente ». Quels sont les enjeux liés aux données dans la « ville intelligente », « l'usine du futur », le monde médical etc. ?

Axe 8 : enjeux sociétaux et éthiques liés aux données.

La transformation numérique, et la croissance exponentielle des données qu'elle génère, constituent à n'en pas douter des opportunités. Mais la rapidité de cette évolution et ses conséquences majeures sur l'Homme militent également pour une certaine prise de recul et un questionnement éthique et philosophique. Au plan individuel, que signifie désormais la notion de « vie privée » ? Est-il également possible de replacer l'utilisateur au cœur de cette transformation en lui permettant de se réapproprier « ses » données ? Faut-il enfin imaginer, sur le modèle de la loi bioéthique, une loi sur l'éthique numérique fixant un cadre pour l'exploitation des données à des fins prédictives ou à des fins de surveillance ?

Réagissez à cet article

Source : *Le FIC 2016 aura lieu les 25 et 26 janvier 2016 sur le thème de la sécurité des données | Observatoire FIC*

Les entreprises françaises bientôt condamnées à changer leur système de traitement des donnée personnelles ?

Les entreprises Françaises bientôt condamnées à modifier leur système de traitement des données personnelles ?

L’échéance se rapproche dangereusement. A partir de la fin du mois de janvier, entreprises américaines et européennes ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Le 6 octobre 2015, la Cour de justice européenne a en effet rendu une décision invalidant le « Safe Harbor », ce traité transatlantique sur le transfert des données personnelles. Premiers touchés, les géants américains du numérique, comme Facebook, Google ou Microsoft, qui exploitent massivement les donnes personnelles.

Qu’en est-il des entreprises françaises qui, sans toujours le savoir, communiquent les données personnelles de leurs clients. De leurs salariés, de leurs contacts… sur des serveurs aux États Unis ? (Gmail, DropBox, Google Drive…)

A partir de la fin du mois de janvier, les entreprises américaines et européennes, et donc françaises, ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.

Vous avez des doutes, vous souhaitez être accompagné ?
contactez-nous

Réagissez à cet article

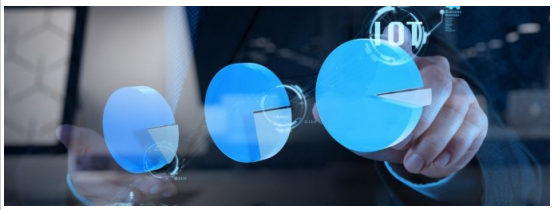
Source : *Fin du « Safe Harbor » : Gattaz tire la sonnette d’alarme*

L’Internet des objets

boostera-t-il l’Europe ?

L’Internet des objets, boostera-t-il l’Europe ?

En plein CES de Las Vegas, AT Kearney vient de livrer une version rafraîchie de son étude sectorielle sur la high-tech en Europe avec un focus #IoT.



L'Internet des objets donnera-t-il un nouveau souffle au secteur high-tech en Europe ? AT Kearney a publié un focus dans ce sens qui montre tout le potentiel…s'il est bien exploité.
En pleine effervescence du CES organisé à Las Vegas, le cabinet de consulting d'origine américaine vient de présenter à Paris la troisième version de son étude sur les nouvelles technologies en Europe sous l'angle de l'IoT
C'est une véritable opportunité de croissance sur les 10 prochaines années, estime Hervé Collignon, Partner d'AT Kearney, expert en TMT (télécoms, médias et technologies) et co-auteur du rapport.
Ce potentiel économique est estimé à près de mille milliards d'euros d'ici 2025. Il pourrait correspondre à 7 points de PIB à cet horizon.
Et les start-up comme Sigfox, Netatmo ou Withings et les groupes industriels français ont une carte à jouer. Ils ont pris position sur le marché des objets connectés dans le BtoC et le BtoB (historiquement via le M2M).
Dressons d'abord le tableau des perspectives présumées gigantesques de cet Internet des objets, qui va permettre « l'interconnexion du monde physique en facteur 10 par rapport à l'Internet phase 1 ».
Entre les technologies exponentielles (capteurs, bande passante, hardware, stockage & cloud), la population connectée (3 milliards de personnes en 2015), les effets réseaux (peering, IPv6, plateformes, interopérabilité…) et l'essor du big data, tous les ingrédients sont réunis pour assister à une « nouvelle révolution » qui va toucher tous les secteurs d'activité, estime Hervé Collignon.
A l'horizon 2025, le marché des solutions IoT en Europe (hors fabrication des objects connectés) est évalué à 80 milliards d'euros. Les intégrateurs de systèmes (IBM, Accenture, Atos…) remporteraient la plus grosse part du gâteau : plus d'un quart du business généré (22 milliards d'euros), devant les fournisseurs de services et de plateformes (le club GAFA et les opérateurs télécoms) qui pourraient en tirer un business de 18 milliards d'euros….
On retrouverait les opérateurs dans une autre catégorie : les spécialistes de la connectivité pour l'IoT. Un segment qui pourrait peser 15 milliards d'euros à l'horizon 2025 et qui comporte des pure players comme Sigfox.
Toujours selon le cabinet en stratégie qui a présenté mardi midi les résultats de son étude à Paris, on devrait recenser dans dix ans une base installée de 26 milliards d'objets connectés (correspondant à un marché de 10 milliards d'euros pour les fournisseurs de composants et modules comme Sierra Networks, Telit ou Gemalto).
L'essor de la dimension Internet des objets devraient avoir un impact sur 5 secteurs principalement : le transport et l'hôtellerie (250 milliards d'euros), la santé (235 milliards d'euros), la domotique domestique (160 milliards d'euros), le matériel industriel (pour un montant similaire), et la distribution, commerce (hors commerce électronique) et vente en gros (60 milliards d'euros).
Divers paramètres pourraient modifier cette perspective apportée par AT Kearney : le niveau d'adoption des objets connectés par les consommateurs, la politique industrielle associée à l'IoT en Europe (balbutiante en l'état actuel malgré une certaine prise de conscience par la Commission européenne), la guerre d'influence des plateformes (Google, Apple, Samsung…), la rationalisation des standards IoT sur fond de consortiums puissants (Open Interconnect, Allseen Alliance, Industrial Internet Consortium…), l'avancée de la 5G en Europe, l'impact de l'IoT sur l'emploi et la juste appréciation du traitement des données.
Etude « The Internet of Things : a new path to European Prosperity », ATKearney, janvier 2016, co-auteurs : Thomas Kratzert et Michael Broquist (respectivement Partner et Principal à Stockholm), Hervé Collignon et Julien Vincent (respectivement Partner et Principal à Paris)
En savoir plus sur http://www.itespresso.fr/europe-vraie-puissance-internet-objets-117702.html#2t626JMWackx6u04.99

Réagissez à cet article

Source : *L'Europe, une vraie puissance de l'Internet des objets ? | ITespresso.fr*

L'aviation civile n'est pas à l'abri du cyber-terrorisme

L'aviation civile n'est pas à l'abri du cyber-terrorisme

A la demande de l'Agence européenne de sécurité aérienne (Aesa), un hacker pourvu d'une licence de pilote d'avion commercial a démontré qu'il pouvait en quelques minutes entrer dans le système de messagerie des compagnies maritimes.

A l'instar des machines industrielles et des objets domestiques connectés, les véhicules et les avions n'échapperont pas aux attaques des cybercriminels. « L'aviation civile doit se préparer aux cyber-risques », prévient d'ailleurs Patrick Ky, le directeur exécutif de l'Agence européenne de sécurité aérienne (Aesa). En poste depuis 2013, ce dernier s'est exprimé lors d'un petit déjeuner organisé par l'association des journalistes de la presse aéronautique et spatiale (Aspae) en octobre dernier. Ses propos ont été rapportés dans de nombreux journaux tels que Les Echos, Le Parisien ou encore l'Usine Nouvelle. Patrick Ky est formel : le piratage informatique d'un avion est possible et la cybercriminalité représente bien une véritable menace pour le transport aérien.

Pour illustrer ses propos, le directeur exécutif de l'Aesa a confié qu'il avait fait appel à un Hacker. Cet expert en informatique – également titulaire d'une licence de pilote d'avion commercial – est parvenu en quelques minutes à entrer dans le système de messagerie Acars (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Lequel sert aux compagnies aériennes à envoyer des messages automatiques et réguliers de l'avion vers le sol pour s'assurer du bon fonctionnement des systèmes critiques de l'avion.
Risque accru. Demain, le risque de cyberattaque va être accru avec la mise en place du système Sesar (Single European Sky ATM Research ; en français : Ciel unique européen) qui vise à harmoniser en Europe le trafic aérien en déployant un réseau et de nouveaux systèmes de gestion d'ici 2025. Ce nouveau réseau européen de contrôle du trafic aérien aura la possibilité de donner directement des instructions aux systèmes de contrôle de l'avion. Pour limiter les risques de piratage, l'agence européenne pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu'elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, Patrick Ky veut mettre en place une structure en charge d'alerter les compagnies aériennes sur les cyberattaques. Un risque sur lequel Air France, que nous avons contacté, ne s'est pas encore publiquement prononcé.

Réagissez à cet article

Source : *L'aviation civile n'est pas à l'abri du cyber-terrorisme*

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Les téléphones cryptés, le casse-tête des enquêtes antiterroristes

Invité à s'exprimer sur France Inter, vendredi 8 janvier, sur les attentats qui ont frappé la France en 2015 et l'attaque, la veille, d'un commissariat du 18e arrondissement de Paris, le procureur de la République à Paris, François Molins, est revenu sur l'une des principales difficultés techniques à laquelle font face les enquêteurs en matière d'antiterrorisme : travailler sur les « téléphones cryptés » retrouvés, dont les codes de verrouillage sont de plus en plus complexes à casser.

« Tous les smartphones qu'on essaie aujourd'hui d'exploiter sont verrouillés et cryptés (…) *toutes les communications passées par les terroristes sont passées à l'aide de logiciel de cryptage »*, a expliqué M. Molins, qui a cependant tu les noms des principaux logiciels utilisés.
« Les évolutions technologiques et les politiques de commercialisation d'un certain nombre d'opérateurs font que si la personne ne veut pas donner le code d'accès on ne peut plus rentrer dans les téléphones », a souligné M. Molins. La totalité des données deviennent ainsi inaccessibles à quiconque ne possède pas le code de déblocage.

PLUSIEURS TÉLÉPHONES N'ONT TOUJOURS PAS ÉTÉ « CASSÉS »

Une difficulté qui rend les enquêteurs *« aveugles »* dans certains cas et les prive de moyens d'investigation, a regretté M. Molins, en citant notamment le cas de Sid Ahmed Ghlam.
L'un des téléphones de l'étudiant algérien soupçonné d'un projet d'attentat contre une église de Villejuif au printemps n'a, en effet, toujours pas été « *cassé* » par les policiers. Mais un iPhone 4S saisi dans le cadre de l'enquête sur le 13 novembre garde également, à ce jour, tous ses mystères.
Dans les jours qui ont suivi les attentats du 13 novembre, la direction centrale de la police judiciaire (DCPJ) a ainsi demandé à tous ses services de résumer les problèmes posés par les *« téléphones cryptés ».« Les téléphones de dernière génération disposent de codes verrous très compliqués à casser ou contourner »*, expliquait au *Monde* le service central de l'informatique et des traces technologiques de la police judiciaire (SCITT) en réponse à la demande de la DCPJ.

De quoi inquiéter ces experts de la police scientifique : *« Les solutions utilisées ne sont pas pérennes, dans la mesure où elles sont basées sur l'exploitation de failles logicielles, le plus souvent corrigées lors des mises à jour. »* C'est le cas de l'iPhone de l'enquête du 13 novembre.

En 2014, sur 141 téléphones analysés par le SCITT, six n'ont pu être explorés. Quant à 2015, *« huit smartphones n'ont pas pu être pénétrés dans des affaires de terrorisme ou de crime organisé »*, a détaillé M. Molins.

Concernant le cryptage, *« il n'existe à ce jour aucune solution permettant aux services techniques de déchiffrer systématiquement les données »*, assure la sous-direction de la lutte contre la cybercriminalité, également sollicitée par *Le Monde*.

UNE ACTION JURIDIQUE POUR REMÉDIER AU PROBLÈME

Deux solutions s'offrent alors aux services d'enquête judiciaire. D'abord faire appel à la direction générale de la sécurité intérieure (DGSI). Mais le centre technique d'assistance du service de renseignement répond dans un délai moyen de trois mois, et sans garantie de succès. De toute façon, reconnaît une source à la DCPJ, *« cette possibilité semble ignorée par de nombreux services »*. Les policiers peuvent aussi, éventuellement, se tourner vers les fabricants, dont certains, comme Apple, acceptent désormais, *« dans le cadre d'une urgence vitale »*, de communiquer les données stockées dans le « cloud ». A supposer qu'une sauvegarde ait été réalisée par le mis en cause.
Autant dire que le pessimisme règne du côté des services d'enquête comme des experts de la police technique et scientifique. *« Il paraît illusoire d'attendre une solution multisupport qui permettrait un accès aux données verrouillées. Seule une action juridique pourrait permettre d'obtenir ces données par le biais d'un instrument légal… Le problème réside cependant dans le poids d'un tel outil juridique face à des opérateurs ou des industriels ayant leur siège à l'étranger »*, conclut le SCITT.

Réagissez à cet article

Source : *Les téléphones cryptés, casse-tête des enquêtes antiterroristes*

Par Laurent Borredon

Est-ce que la réutilisation de données personnelles sera possible dans le nouveau

Règlement vie privée ?

	Est-ce que la #réutilisation de données personnelles sera possible dans le #nouveau Règlement vie privée ?

Tout praticien de la protection des données personnelles a déjà été confronté au problème du changement de finalité d'utilisation des données. Exemple : elles ont été collectées pour une finalité d'exécution d'un service en ligne (accès à un réseau social ou livraison d'un bien acheté) et on voudrait aujourd'hui les vendre en vue d'alimenter une processus de profilage big data. Les conditions de pareils changements de finalité ont divisé les juristes et organes de contrôle depuis la directive de 1995. Le nouveau règlement semble avoir tranché : la poursuite d'une nouvelle finalité incompatible avec la première est interdite, sauf consentement préalable des personnes concernées.

La problématique

On ne peut pas savoir au moment de la collecte des données personnelles à quoi elles pourront servir dans quelques mois ou années. Surtout dans un contexte d'évolution technologique permanente et de plus en plus rapide.

Le gestionnaire des données est donc un jour ou l'autre tenté d'utiliser les données en sa possession, pour une finalité autre que celle annoncée initialement. Du reste, on rappelle que s'il n'utilise plus les données, le gestionnaire doit les effacer après une période qui dépend de la finalité de départ. Choix cornélien donc : soit j'efface les données si je reste dans la finalité de départ et que celle-ci a été exécutée, soit je les réutilise pour une nouvelle finalité si je souhaite conserver les données.

Les processus de Big data offrent un parfait exemple de la problématique. Les outils de profilage demandent par définition de se nourrir de très nombreuses observations issues de traitements de données divers et variés. La plupart du temps, ces traitements n'ont pas été mis en œuvre pour permettre un processus de profilage. Cette finalité n'était pas prévue initialement (par exemple, l'inscription et la gestion d'un jeu en ligne sur internet ; l'inscription et l'utilisation un site d'échanges en vue de vendre certains biens etc.). La nouvelle finalité est souvent incompatible avec la première et, selon les lois sur la protection des données personnelles, elle est a priori interdite.

Deux interprétations semblaient s'affronter :

• Soit on considérait que la nouvelle finalité incompatible ne pouvait être poursuivie qu'à la condition de recueillir le consentement de la personne concernant la nouvelle finalité d'utilisation des données. Dans notre exemple, le responsable qui veut se relancer dans son projet Big data, doit réinterroger chaque personne afin d'obtenir son consentement explicite sur la nouvelle finalité d'utilisation.

• Soit on admet y voir un nouveau traitement pouvant être poursuivi comme tel, c'est-à-dire en le soumettant à l'intégralité de la protection légale (information des personnes concernant la nouvelle finalité, nouvelles mesures de sécurité ou de sauvegarde si nécessaires, détermination d'une nouvelle base de licéité qui n'est pas forcément le consentement de la personne mais par exemple un équilibre d'intérêts avec droit d'opposition, nouvelle déclaration auprès de l'autorité de protection des données etc.). Cette deuxième opinion, plus souple, permet d'admettre une évolution inévitable des finalités d'utilisation, tout en garantissant les droits et libertés de la personnes.

Le système sévère du futur Règlement

La disposition finale du projet de Règlement ne comprend plus aucune disposition concernant le problème du changement de finalité et les conditions dans lesquelles il aurait pu intervenir.

L'évolution du texte témoigne d'un véritable débat sur ce point.
Le texte initial ne contenait aucune règle spécifique.

La seconde version a introduit un nouveau paragraphe ayant cet objet (article 6§4). Si les données étaient collectées par le même responsable du traitement, la poursuite d'une finalité ultérieure aurait été permise malgré l'incompatibilité des finalités, pour autant que l'on ait pu justifier celui-ci par une des hypothèses générales de licéité prévue au §1er(consentement, exécution d'un contrat, intérêt vital de la personne etc.).

En d'autres termes, selon la deuxième version du texte, le responsable aurait toujours pu remédier à une incompatibilité entre la finalité initiale et les finalités ultérieures du traitement, en identifiant une nouvelle base de licéité du traitement. En fin de compte, le responsable pouvait toujours prendre le risque de fonder la licéité du nouveau traitement sur la fameuse balance des intérêts, et gérer les soucis a posteriori.

La dernière version du Règlement, ayant fait l'objet du dernier vote en commission, a purement et simplement retiré ce paragraphe.

Le Groupe Article 29 a donc obtenu satisfaction, lui qui avait fortement critiqué cette disposition qui, à ses yeux, mettait à mal et vidait de sa substance le principe de finalité (cfr. Article 29, Opinion 03/2013 on purpose limitation, 2 avril 2013, p. 36 et 37).

Le principe de base est dès lors celui de l'exigence de la compatibilité des finalités nouvelles avec les finalités initiales, sauf consentement de la personne concernée ou un texte légal spécifique le permettant pour des finalités spécifiques (sécurité nationale, défense, sécurité publique etc.) En cas d'incompatibilité, la poursuite de la finalité incompatible est donc prescrite et le changement de finalité rendu illicite.

Des conséquences pratiques importantes

Le Règlement choisit donc la sévérité concernant le régime de changement des finalités.

L'interdiction de traitement en cas d'incompatibilité des finalités s'oppose à l'évolution d'un traitement de données qui est en quelque sorte « figé » par sa finalité réelle de départ. Si des données ont été traitées pour les besoins d'exécution d'un contrat, elles ne pourront la plupart du temps pas être traitées pour une communication à un tiers en vie d'alimenter un processus de profilage big data car ce sera considéré comme finalité incompatible, sauf à obtenir a posteriori le consentement de chacune des personnes concernées.

Sans aller jusqu'à autoriser le changement de finalité sans garantie particulière, un moyen terme était possible si on était parti du principe que la seconde finalité générait un « nouveau » traitement qui devait être soumis au respect de l'intégralité des dispositions de la loi (nouvelle information des personnes, identification d'un nouveau critère de licéité, identification des mesures de sécurité spécifiques, le cas échéant, etc.) et pas seulement à la seule exigence de la licéité.

La solution du Règlement est autre : on ne peut pas modifier une finalité annoncée sans le consentement préalable de la personne. Ce qui pose non seulement problème pour le traitements futurs mais aussi question pour les traitements antérieurs ou qui seront en cours au moment de l'entrée en vigueur du futur Règlement. Le Règlement ne prévoit en effet pas de régime transitoire.

Réagissez à cet article

Source : *Nouveau Règlement vie privée : la réutilisation de données sera-t-elle encore possible ?*

Vol et fuite de données, comment les éviter ?

Vol et fuite de données, comment les éviter ?

Les données, tout le monde le sait désormais, sont d'une importance capitale et d'une valeur inestimable. En tant qu'entreprise, comment les valoriser et surtout comment bien les protéger ?

Et si vous possédiez déjà l'argile des futurs développements de votre entreprise ? En effet, en travaillant les données récoltées par les différents services de votre société, vous pouvez déjà optimiser vos produits et services actuellement commercialisés notamment via l'analyse des données liées à la satisfaction des clients. Mais, plus encore, vous pouvez également faire évoluer vos produits et services voire en créer de nouveaux. **L'étude des data permet de comprendre les usages et de modifier les produits et services en fonction de ces usages**.
Citons les statistiques sur les données révélant les besoins des usagers des transports publics. Citons plus précisément la compréhension des verbatims-clients grâce au logiciel d'analyse sémantique de Dictanova. Citons encore les données issues de l'analyse des cultures agricoles récoltées par les sondes de Weenat.

Déclaration à la CNIL obligatoire

Pour réussir parfaitement cette utilisation, certaines précautions doivent être prises et en tout premier lieu, lorsque votre base de données contient des données personnelles, il est absolument nécessaire de procéder au préalable aux déclarations CNIL (simplifiées, normales voire demande d'autorisation). Outre les potentielles sanctions administratives et pénales, un fichier non déclaré est considéré comme illicite et ne peut donc être ni vendu ni loué. Les juges ont clairement déclaré qu'**un tel fichier non déclaré constituait un objet illicite, hors commerce, insusceptible d'être vendu** (Com. 25 juin 2013). Rappelons également que l'introduction dans un fichier d'une donnée personnelle nécessite le consentement éclairé et préalable de la personne concernée.
Mais, la Data, c'est également une multitude d'informations qui n'ont aucun rapport avec les données personnelles. On peut les appeler « données objectives » ou « données brutes ». Or, au cœur de votre entreprise, il y a aussi de telles informations qui sont certes, plus ou moins organisées. Sachez qu'une fois optimisée en base de données, la data est une véritable mine d'or.

Droit d'auteur ou droit du producteur ?

En organisant vos données, vous valorisez à la fois le contenu (la data) et le contenant (la ou les bases de données). La base de données peut être protégée par le droit d'auteur si le choix ou la disposition des matières constitue une création intellectuelle originale c'est-à-dire lorsque son auteur ou son concepteur fournit un effort personnalisé, éloigné de toute logique automatique et contraignante (cf. article L112-3 du Code de la propriété intellectuelle).
La base de données peut également être protégée via la reconnaissance de la qualité de **producteur de bases de données**. Ici, il s'agit de démontrer en particulier le risque des investissements sur la base de données lors de sa constitution, sa vérification ou sa présentation : investissement financier, matériel ou humain substantiel relevant des moyens consacrés à la recherche de données existantes, à leur rassemblement et le suivi de la base (cf. article L341-1 du Code précité).
Par conséquent, droit d'auteur ou droit du producteur de base de données, vous pouvez être titulaire d'un véritable droit de propriété sur vos données via l'existence de véritables bases de données.
A ce titre, vous pouvez vous en **réserver l'exclusivité** et délivrer à vos clients des prestations de service ou des licences d'utilisation, issues de l'exploitation des données. La seule réserve dégagée par les juges est l'abus de position dominante de telle manière qu'un monopole sur certaines données ne doit pas être préjudiciable aux autres acteurs économiques (Com. 4 décembre 2001 – France Télécom et son fichier d'abonnés).
Sans l'organisation de la data au sein de bases de données, votre data est de libre parcours. Elle relève du bien commun. Titulaire d'un droit de propriété intellectuelle, vous pouvez interdire certaines formes d'extraction et d'utilisation du contenu de votre base et donc de votre data. Dans ces conditions, invoquer un acte de contrefaçon est plus aisé que de démontrer un acte de concurrence déloyale ou de parasitisme.
Parce qu'une fois organisées, les données de votre entreprise ont de la valeur, il faut cultiver votre data, sans trop dénaturer la maxime de Voltaire « Il faut cultiver notre jardin » !

Réagissez à cet article

Source : *Startup : Comment bien protéger sa data, ce précieux patrimoine immatériel ? – Maddyness*

Par Marie-Pierre L’hopitalier, avocat associé.

Crédit photo : Shutterstock