# ZATAZ 93 millions d’électeurs Mexicains accessibles sur la toile – ZATAZ

| | |
|---|---|
|  | 93 millions d’électeurs Mexicains accessibles sur la toile |

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

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

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

---



Réagissez à cet article

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

---

# La Grande Loge de France victime d’une fuite de données massive

| | |
|---|---|
|   | La Grande Loge de France victime d’une fuite de données massive |

---

**La Grande Loge de France (GLDF) a porté plainte contre X pour #piratage informatique le 12 avril 2016 après la découverte d'un logiciel espion dans son réseau informatique. Fuite de données massive constatée.**


C'est dans le blog « *La lumière* » hébergé par l'Express que l'information est sortie. La Grande Loge de France (GLDF) a porté plainte contre X pour piratage informatique le 12 avril 2016 après la découverte d'un logiciel espion dans son réseau informatique.
Toute l'histoire a débuté le 2 avril. Un code malveillant est introduit dans l'informatique de la GLDF. 48 heures plus tard, les informaticiens de La Grande loge tire la sonnette d'alarme. Un malveillant est passé par là. Il aurait réussi à atteindre le cloud de l'administration des Francs-maçons. Il semble qu'un cheval de Troie (ou tout simplement un phishing) a permis de mettre la main sur l'accès à ce « *nuage*« . Un cloud, qui faut-il le rappeler est le diable si le contenu des informations sauvegardées ne sont pas chiffrées, contenait des milliers de documents internes.

**Fuite de données massive**

Le pirate a diffusé l'ensemble des documents, sur son blog, le 10 avril, sous le nom de « *Franc Maçons Papers*« . Trouble et étonnante histoire. L'auteur de ce piratage et de sa diffusion ne se cache pas. Il parle même de « ***La plus grosse fuite de documents secrets de l'Histoire de France***« . Il faut dire aussi qu'avec près de 3 Go de données, que j'ai pu constater, la fuite n'est pas légère. A suivre !… [Lire la suite]

---

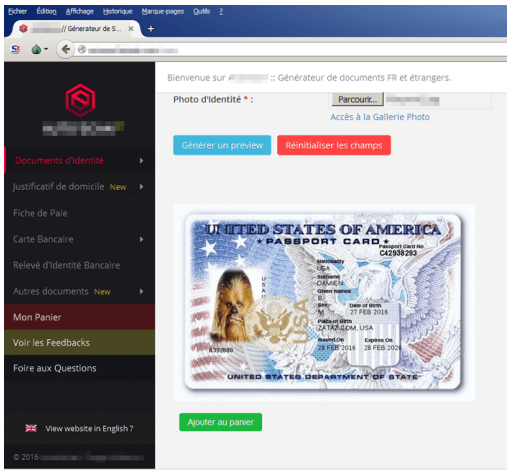


Réagissez à cet article

Source : *ZATAZ Fuite de données massive après un piratage chez les Francs-Maçons – ZATAZ*

---

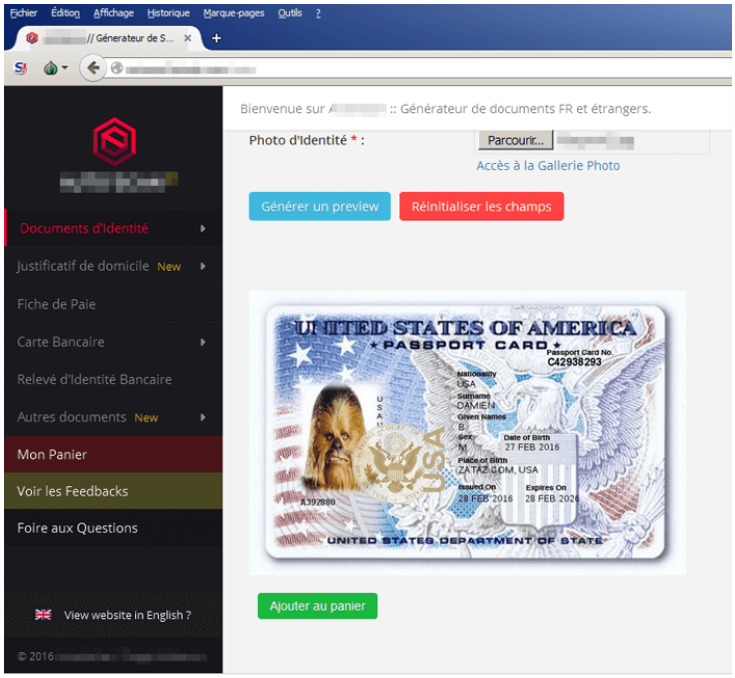
# Le Darknet cache un générateur de faux documents




**Le Darknet cache un générateur de faux documents**

---

**Vous cherchez de faux documents comme un diplôme du baccalauréat, de BTS ? Une fausse facture FREE, EDF, Direct Énergie ? Un faux permis de conduire ? Une fausse fiche de paie ou une fausse carte bancaire ? Un site Internet vous propose d'automatiser l'usurpation.**




Ils sont de petites stars dans le black market, deux francophones devenus des références dans la contrefaçon de documents. Les autorités leurs poseraient bien deux/trois questions, mais les deux administrateurs du portail A.S. [Le nom a été modifié, NDR] sont malins, cachées dans les méandres du darknet. Leur site, pas la peine de me réclamer l'adresse, est caché sous une adresse .onion. A.S. profite de l'anonymat proposé par le service TOR pour éviter d'afficher ouvertement son serveur, son ip d'origine. Et même si vous mettiez la main sur ce dernier, l'hébergement est hors de l'hexagone.

« ***Bienvenue sur A'S. :: Générateur de documents FR et étrangers*** » souligne l'introduction affichée par le site. Mission de ce dernier, pour quelques euros, facturés en Bitcoins, générer de fausses factures, fausses fiches de paie, faux relevé d'identité bancaire (RIB). Il est possible de générer un faux diplôme du Baccalauréat, de BTS, d'IUT. Une fausse carte vitale ? Pas de problème. Une facture d'un achat effectuée chez Darty, ok. Passeport Français, Américain et autres copies d'une carte nationale d'identité boucles ce service… qui n'a rien d'illégal, du moins si vous rentrez vos propres coordonnées. Il en va tout autrement si les informations que vous fournissez permettent d'usurper une identité, une fonction, un titre via ses faux documents. La loi punit de trois ans d'emprisonnement et de 45000 euros d'amende le faux et l'usage de faux documents.
Les prix varient de 4,99€ pour une copie de passeport, une facture. 9,99€ pour le scan d'un bulletin de fiche de paie. 6,99€ pour la copie d'un diplôme du baccalauréat général. Les auteurs de ce business proposent même un abonnement à vie. Pour ~~79 800~~ euros, les commerciaux indiquent permettre « ***un accès illimité et à vie à tous les articles de cet Autoshop pour 200€ ~~BTC~~***« . La boutique annonce un anonymat garanti. [Correction : selon les auteurs, il s'agit de 200€ et non 200 BT comme il était écrit sur leur site, NDR]… [Lire la suite]

---

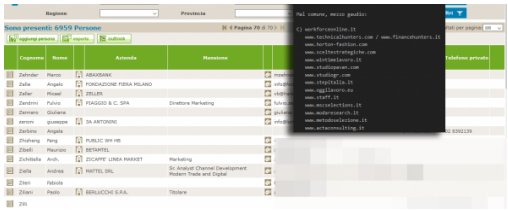


Réagissez à cet article

Source : *ZATAZ Générateurs de faux documents – ZATAZ*

---

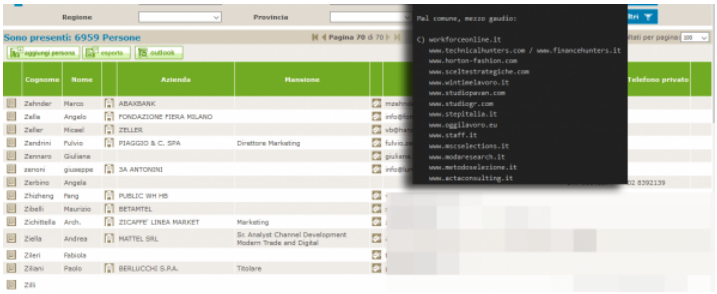
# Des milliers de données clients diffusées sur Internet par Anonymous



Des milliers de données clients diffusées sur Internet par Anonymous

---

**Données clients diffusées sur Internet – Des internautes ont lancé, sous la signature Anonymous, une opération contre le business des laboratoires pharmaceutiques. Ils veulent dénoncer « les porcs et les connivences entre les gouvernements et les sociétés« . En Italie, c'est un hébergeur qui fait les frais d'une cyber action.**




Étonnante revendication que celle lancée par les Anonymous. Lundi 11 avril, des internautes ont lancé un appel pour cibler « ***les porcs et les connivences entre les gouvernements et les sociétés pharmaceutiques***« . Pour les organisateurs, la mission est de collecter des informations, des données, pour les diffuser ensuite. « ***Nous voulons dire la vérité sur le cancer, la nutrition, les médicaments…*** » indique les personnes cachées derrière la signature et le masque Anonymous. « ***Notre santé est plus importante que leur profit !*** […] ***Beaucoup d'entre vous ont déjà pris conscience de ce système axé sur les profits, il est temps de prendre des mesures, il est temps d'exposer la corruption et demande justice pour les victimes*** ».

**En Italie, des données clients diffusées sur Internet**

En Italie, l'agence web Engitel, basée à Milan, se faisait pirater et voler plusieurs milliers de données par Anonymous Italia et un second groupe du nom de LulzSecITA. 40 sites impactés, plus de 2 800 fichiers sensibles ont d'abord été diffusés. Ici pas d'attaque SQL, mais ce qui semble être une copie conforme des données clients, et leur site web, via l'espace d'administration de l'entreprise Milanaise.

Anonymous Italie, la source initiale de la fuite, a affirmé qu'il y avait plus de 1,8 millions de données d'utilisateurs. Ils vont le prouver en diffusant plusieurs autres dossiers, via MEGA. Dans l'un des dossier que j'ai pu consulter, des fichiers qui permettent de contacter les responsables des sites Internet (J'ai pu en dénombre 6 959) de sociétés italiennes telles que MTV Italie, La Repubblica, Facebook Italie, Gucci, FastWeb, Microsoft, Wind, Ducati… « ***Voici notre premier chapitre de notre opération Nessun Dorma,*** indique les hacktivistes. ***Nous sommes fatigués des mensonges habituels diffusés dans tous les médias au sujet du monde du travail*** ».

Bref, comme l'indiquent les pirates dans leur – communiqué de presse – : Si vous voulez la paix, préparez la guerre. A noter que plusieurs sites Suisses (aiti.ch, e-lavoro.ch, aitiservizi.ch, e-impresa.ch, jobopportunity.ch, BFKconsulting.ch, helvia.ch et workandwork.ch) ont été piratés lors de cette opération… [Lire la suite]

---



Réagissez à cet article

Source : *ZATAZ Anonymous : des milliers de données clients diffusées sur Internet – ZATAZ*

---

# WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

---

**C'est peut-être l'absence de prise en compte de patchs de sécurité pour un plug-in WordPress et pour le CMS Drupal qui aurait permis de récupérer chez Mossack Fonseca les fameux Panama Papers qui font trembler le monde de la finance.**

La fuite massive des documents de Mossack Fonseca, le cabinet panaméen qui gère des compagnies offshores, n'a pas fini de faire parler d'elle. Les 11,5 millions de documents contenus dans les 2,6 To de données – les fameux Panama Papers – ont déjà ébranlé de nombreuses sociétés et les sphères politiques, poussant par exemple le Premier ministre de l'Islande à démissionner. Mais comment ces données ont-elles été obtenues ?

## NÉGLIGENCE INFORMATIQUE

De nombreuses questions demeurent concernant l'origine de la fuite qui provient d'une source anonyme. Mais beaucoup s'accordent sur le fait que la sécurité informatique a été négligée par Mossack Fonseca, ce que le cabinet avoue à demi mots en portant plainte pour piratage informatique.

Dans un mail qu'il ne fallait pas prendre pour un poisson d'avril, le cabinet avait expliqué à ses clients dès le 1er avril qu'il avait été victime d'une « brèche non autorisée de [son] serveur mail », comme le montre une copie publiée par Wikileaks le 3 avril. Bien sûr, les réactions sur Twitter ne se font pas fait attendre, amusées par la date d'envoi du mail et par l'absence de chiffrement des courriers électroniques de la part d'une entreprise qui met en avant « ses prestigieux services en ligne », comprenant « un compte sécurisé qui vous permet d'accéder n'importe où aux informations de votre société ».

## DE L'IMPORTANCE DE METTRE À JOUR DRUPAL ET WORDPRESS

De récentes informations corroborent la thèse du piratage, qui aurait pu être facilitée par des vulnérabilités au sein des CMS utilisés par Mossack Fonseca, à savoir les gestionnaires de contenus Drupal et WordPress.

Comme le rapporte Forbes, le portail client du cabinet fait tourner une vieille version de Drupal (7.23). Or cette version est antérieure à un patch de sécurité qui corrigeait une énorme faille à partir de la version 7.32. Dans une notice de sécurité, Drupal allait jusqu'à recommander une nouvelle installation aux utilisateurs n'ayant pas mis à jour immédiatement après la sortie du correctif.

Il se peut donc qu'un attaquant ait exploité cette faille durant les deux années pendant lesquelles le cabinet n'a pas mis à jour sa version du CMS. Mais d'autres experts en informatiques ont découvert une autre porte qui aurait pu permettre à un hacker d'entrer dans le système.

Si le portail client du cabinet est sous Drupal, le site principal est lui sous WordPress. L'entreprise Wordfence, spécialisée dans la sécurité de l'omniprésent gestionnaire de contenus, a remarqué que l'installation WordPress utilisait une ancienne version du plugin Revolution Slider, connue pour présenter une faille sérieuse.

La version 3.0.95 de Revolution Slider (et les versions antérieures) contiennent en effet une vulnérabilité qui permet à un assaillant d'envoyer un fichier sur le serveur web sans avoir à s'identifier. L'entreprise note qu'un attaquant aurait donc pu prendre le contrôle du serveur sur lequel se trouvait l'installation WordPress… Le même serveur qui hébergeait les très précieux e-mails du cabinet.

En l'occurrence, rien ne prouve que les failles au sein des installations WordPress et Drupal du cabinet aient facilité la fuite des données. Dans la mesure où les journalistes n'ont pas rendu publics les documents, il sera d'ailleurs difficile de déterminer d'où ils proviennent. De son côté, le cabinet affirme qu'il s'agirait d'une attaque effectuée depuis l'étranger, écartant par la même toutes idées de fuites internes.

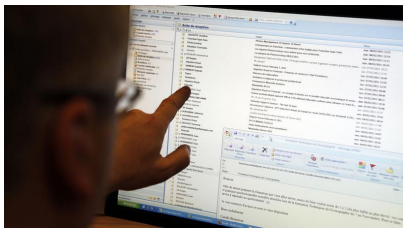
… [Lire la suite]

---



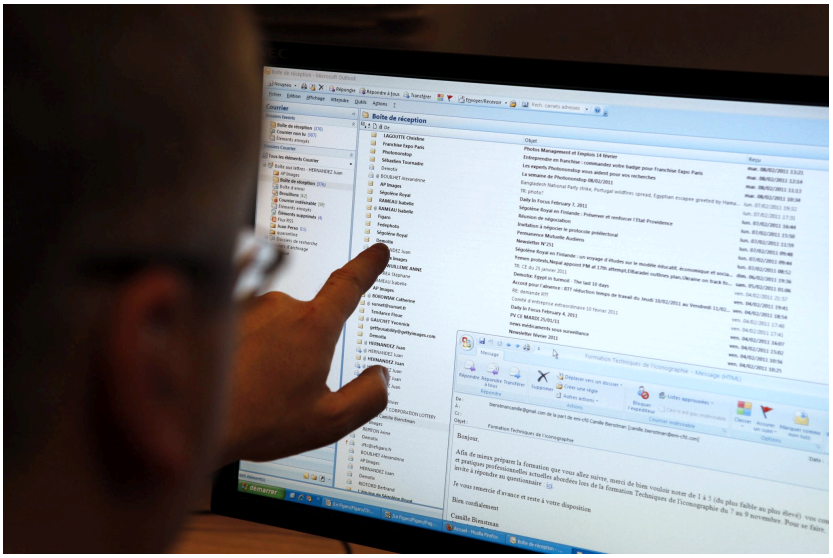
Source : *Panama Papers : des WordPress et Drupal mal gérés à l'origine d'un piratage ? – Tech – Numerama*

# 100 fois plus de victimes vol de données personnelles en deux ans en France



100 fois plus de victimes vol de données personnelles en deux ans en France

**En 2015, cette pratique visant à dérober des informations personnelles par Internet ou par téléphone a fait plus de 2 millions de victimes en France. C'est cent fois plus qu'il y a deux ans.**



Véritable piège pour les internautes, la pratique du phishing ne cesse de se répandre en France. Contraction de «fishing» (pêche) et «phreaking» (piratage de lignes téléphoniques), ce procédé malveillant vise à soutirer des données personnelles (mot de passe, identifiant de connexion, numéros de cartes bancaires). On parle également de «hameçonnage».

Sur la seule année 2015, plus de 2 millions de personnes auraient été victimes du phishing en France. C'est 100 fois plus qu'il y a deux ans, selon Europe 1 qui reprend un rapport de Phishing Initiative, site reconnu par les services de lutte contre la cybercriminalité. Le plus souvent, cette arnaque se manifeste par la réception d'un mail personnalisé provenant d'un organisme financier (banques), d'une entreprise (fournisseur d'Internet, EDF…) ou même d'une administration publique (CAF)… Du moins en apparence.

Car le message en question, aussi crédible et réaliste qu'il puisse paraître, vous invite en réalité à cliquer sur un lien, lequel vous redirige vers un site vous demandant de mettre à jour vos données personnelles. Dès lors, en se faisant passer pour des tiers, les cybercriminels à l'origine de ces mails frauduleux sont en mesure de récupérer vos informations personnelles. «L'augmentation des pratiques de phishing s'explique notamment par le nombre croissant de cybercriminels organisés en réseaux très structurés. D'autant que leurs méthodes sont de plus en plus sophistiquées. Auparavant, des fautes d'orthographe présentes dans les mails permettaient d'éveiller les soupçons. Désormais, c'est plus dur à déceler car ils paraissent davantage crédibles», explique Raphaël Renaud, spécialiste des questions liées au phishing.

Usurpées, les banques comme les grandes entreprises sont, elles aussi, directement concernées par le phishing. En modernisant leurs systèmes de sécurité, elles parviennent parfois à contrer les menaces. C'est le cas de Google qui a bloqué 7000 sites utilisés pour des attaques de phishing en 2015. De leur côté, les établissements bancaires assurent «un service de veille et donc une certaine publicité pour prévenir leurs clients, mais celle-ci est souvent insuffisante», remarque Serge Maître, secrétaire général de l'Association Française des Usagers des Banques (AFUB), avant de souligner que «le cryptogramme et le 3D Secure ont montré leurs limites face aux attaques de phishing.»

## Comment réagir face au phishing?

S'il n'est pas encore trop tard, plusieurs méthodes permettent de contrer le phishing. Dans un premier temps, il est préférable de disposer d'un antivirus performant. Ensuite, «l'ultime chose à faire est de ne jamais cliquer dans un lien provenant d'un e-mail. Les services sérieux (banque, opérateurs téléphoniques, etc…) ne vous demandent jamais de changer un mot de passe de cette manière», explique Raphaël Richard avant d'ajouter «qu'il faut directement se connecter sur le site officiel pour ne pas avoir de doute». Enfin, certains sites tels que ou Phishing Initiative permettent de faire vérifier un mail en cas de soupçon mais également de signaler des adresses qui semblent suspectes.

En revanche, si un internaute vient d'être victime de phishing, il doit «déposer plainte si possible devant une brigade spécialisée dans les 48 heures car au-delà, cela devient plus compliqué. Il faut également contacter … [Lire la suite]

---

Réagissez à cet article

Source : *Données personnelles : le nombre de victimes de vol multiplié par 100 en deux ans en France*

---

# Ne donnez jamais une donnée personnelle de santé à un assureur


**Ne donnez jamais une donnée personnelle de santé à un assureur**

---

**Quand il s'agit de données personnelles de santé, les Français ne doivent rien communiquer aux assureurs, aux banquiers ou aux employeurs. C'est le conseil de Philippe Douste Blazy, ancien ministre de la santé, et désormais créateur de la startup Honestica.**


**Les laboratoires pharmaceutiques à voir**

Il a pris la parole lors de l'événement Keynote 2016 organisé par Maddyness le 20 janvier à Paris. "Il ne faut jamais donner de données personnelles aux assureurs, aux employeurs, aux banquiers," dit-il, "les laboratoires pharmaceutiques, il faut voir," ajoute-t-il.

Il parle alors de données personnelles. Il est plus ouvert pour l'usage de données de santé anonymisées. L'ancien ministre est revenu sur son expérience du dossier médical personnel. "Le DMP est le plus grand échec de ma vie quand j"étais ministre de la santé en 2004" déclare-t-il. Il croyait pourtant en ses vertus qu'il s'agisse d'accélérer les diagnostics, de détecter les risques liés à certains médicaments ou de réduire les coûts médicaux.

"En France, on dépense 30 milliards d'euros par an en examens redondants," pointe-t-il. "Vous vous blessez, on va vous faire faire une radio, et si vous devez aller à l'hôpital, on va refaire cette radio, on ne tient pas compte de la radio que vous avez faite dans le privé," illustre-t-il.

**Mediator et sclérose en plaques**

"Avec le DMP, on aurait vu en quelques mois et pas en années, que le Mediator créait des effets indésirables," souligne-t-il. "De plus, on avait dit que la vaccination contre l'hépatite B créait des risques de sclérose en plaques, on aurait vu que c'est faux grâce au DMP," martèle-t-il.

Depuis, il pense faire renaître ce dossier au sein de sa startup Honestica, où il est associé à Frank Le Ouay, l'un des cofondateurs de Criteo. "La création d'un dossier médical personnel a échoué chez les Américains parce qu'ils partent du patient, il faut partir du médecin, c'est lui qui dans le cadre de la relation de confiance avec le patient va pousser cette solution. Mais il faut lui vendre ce dossier médical comme un moyen de gagner du temps, une heure par jour, et pas comme de la paperasse supplémentaire," recommande-t-il.

**Expérimentation en mars**

Sa société va débuter l'expérimentation en mars prochain de sa solution auprès d'un hôpital toulousain. "Les comptes rendus de sortie de l'hôpital sont encore envoyés par la Poste," dit-il, "nous proposons de les gérer électroniquement." Et il mise sur les médecins hospitaliers pour faire le succès de ce dossier médical électronique.

---

Réagissez à cet article

Source : *Philippe Douste-Blazy : "ne donnez jamais une donnée personnelle de santé à un assureur" | La Revue du Digital*

# 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*

---

# 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*

---

# 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