Les moyens de preuves sur Internet | Le Net Expert Informatique

Les moyens de preuves sur Internet

La récente décision de la Cour d'appel de Paris du 9 octobre 2015 rappelle une fois de plus le caractère essentiel de constituer des preuves valables avant d'agir en justice, particulièrement sur Internet. En l'espèce, la société éditrice du site « Onvasortir.com » attaquait en parasitisme la société éditrice du site « dailyfriends.com » pour avoir copié le plan, la structure, les fonctionnalités, l'agencement des rubriques et le contenu de son site internet.

Afin de rendre sa décision, la Cour s'est appuyée sur des copies écran (des sites en question et d'un forum de discussion), dont la valeur probante était contestée par la partie adverse, mais que la Cour a jugé recevable dans la mesure où elles étaient « parfaitement nettes et datée ». En revanche, la Cour a rejeté un constat d'huissier du fait que l'officier ministériel avait dissimulé son identité lors de ses constats en se connectant aux sites via le compte de la société.
Que ce soit pour un site internet ou une application sur smartphone, la constitution de preuves, souvent difficiles à obtenir et pas toujours recevables, est pourtant essentielle à :
La caractérisation du délit (et donc la condamnation) ;
L'évaluation du préjudice (et donc des dommages-intérêts).

Si la preuve est libre en matière de concurrence déloyale ou de contrefaçon, toutes les preuves ne sont pas admissibles, comme en atteste cette décision, et leur force probante variable. Cet arrêt est donc l'occasion de revenir sur les règles en la matière, avec la particularité de la preuve sur Internet.

I – Les moyens de preuve irrecevables

Au préalable, il n'est pas inutile de rappeler que seules les preuves « légalement admissibles » pourront être retenues devant un tribunal.
Ainsi, il faut entendre par « légalement admissible », les preuves qui ne relèvent pas d'une obtention irrégulière telles que : les écoutes téléphoniques, la violation du secret des correspondances, la réalisation d'un constat en dehors des heures légales ou encore l'atteinte à un principe fondamental tel que la vie privée, le secret professionnel ou le secret de fabrique.
Ainsi, la Cour de cassation, par un arrêt de principe en son assemblé plénière du 7 janvier 2011 a énoncé que « l'enregistrement d'une communication téléphonique réalisé à l'insu de l'auteur des propos tenus constitue un procédé déloyal rendant irrecevable sa production à titre de preuve ».

C'est également sur ce fondement que dans sa décision la Cour d'appel a rejeté le constat dressé par l'huissier de justice qui n'a pas dévoilé son identité en se connectant au site mais a utilisé les identifiants de compte d'un tiers.

II – Les moyens de preuves sur Internet

Il existe plusieurs moyens de preuves visant à faire constater un usage sur Internet dont la force probante est plus ou moins importante.

A) Le constat d'huissier

Une fois établie et validée, cette preuve a une grande force probante.
Ainsi, l'huissier peut procéder à des constations sur Internet à la requête des particuliers. Il a cependant un rôle de simple observateur puisqu'il doit se borner à effectuer des constations purement matérielles.

Le constat sur Internet a cependant posé la question des limites de ce qu'il pouvait constater.
Constat d'un site internet ou d'une application sur smartphone : Sous réserve de respecter certaines conditions techniques (vider le dossier cache du navigateur, absence de serveur proxy…), l'huissier peut faire une description des sites internet accessibles au public, et notamment des produits argués de contrefaçon, et des captures écran des pages du site.

Constat d'achat sur internet : Cette pratique a posé certaines questions en cas de commande sur internet par l'huissier de produits litigieux.
Certains arrêts avaient admis qu'un huissier puisse commander un produit sur un site internet afin d'établir un constat d'achat aux vues de constituer une preuve de la contrefaçon. Cependant, des arrêts, plus récents [1] ont contesté la licéité de cette pratique au motif que l'huissier s'était engagé activement par l'ouverture d'un compte client et l'acquisition du produit litigieux, et avait ainsi outrepassé ses pouvoirs de simple constatation.

C'est en ce sens que va l'arrêt du 7 octobre 2015, qui a dénié toute validité au constat d'huissier qui n'avait indiqué ni sa qualité ni son identité en se connectant au site.
Pour acheter un produit sur internet, l'huissier doit impérativement et comme en matière de constat achat dans les magasins, décliner de manière claire et visible son identité et sa qualité avant de procéder à un acte d'achat. Certaines décisions ont cependant, admis que le seul fait de faire libeller la facture au nom de l'huissier était suffisant pour identifier l'huissier [2].

Sauf à y être expressément autorisé, l'huissier n'a pas le droit d'ouvrir un compte client et, d'acquérir à dessein, un produit allégué de contrefaçon [3].
Le site internet est assimilé à un magasin, comme un lieu privé et, sans autorisation du juge, l'huissier ne peut procéder à ses constatations que depuis la voie publique. Peut-être pourra-t-on procéder comme en matière de constat d'achat en magasin c'est-à-dire, faire procéder à l'ouverture d'un compte client par un tiers sous surveillance de l'huissier qui constatera les démarches effectuées dans le but d'acheter le produit incriminé ? Il faudra également que l'huissier soit présent lors de la réception du colis…ce qui complique les choses.

B) Le constat par un agent assermenté

Il consiste en la description par un agent assermenté d'un acte de contrefaçon. Il pourra être demandé à l'Agence pour la Protection des Programmes (APP) qui dispose d'agents assermentés.
Ce moyen de preuve est particulièrement utilisé en matière de droit d'auteur et de droits voisins et a été admis en matière de propriété industrielle. Ces constats peuvent servir à contourner la difficulté des achats sur internet effectués par un huissier.
Néanmoins, ces constats n'ont pas la force probante des constats effectués par un officier ministériel, et sont par conséquent soumis à l'appréciation souveraine du tribunal.

C) La copie-écran

Enfin, la copie-écran peut également être pertinente même si elle a une force probante moindre, elle représente une bonne solution pour étayer un constat d'huissier ou lorsqu'un constat d'huissier est invalidé comme dans la présente décision du 9 octobre 2015.

Il est donc impératif de connaître les limites d'investigations de l'huissier pour ne pas se voir déclarer irrecevable le constat. Le droit, à l'origine applicable à la vie réelle, essaie tant bien que mal de s'adapter aux contraintes et aux particularités du monde virtuel, et les constats d'huissier ne font pas exception. Attention donc à bien connaître ces spécificités avant d'intenter toute action au fond !

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Source : http://www.village-justice.com/articles/Les-moyens-preuves-sur-Internet,20821.html
Colombe Dougnac – Conseil en Propriété Industrielle

En France, les cyber-attaques sur les entreprises explosent | Le Net Expert Informatique

	En France, les cyber-attaques sur les entreprises explosent

Les entreprises françaises ont subi en moyenne 21 incidents de cybersécurité par jour en 2015. C'est 51% de plus qu'il y a un an selon une étude mondiale du cabinet PwC.

La menace représentée par les cyberattaques sur les entreprises se précise alors que le gouvernement va présenter avec l'Anssi (Agence nationale de la sécurité des systèmes d'information), une charte pour la sécurité des emails signée par cinq fournisseurs de services de messagerie, une étude mondiale révèle l'ampleur du problème.
Selon l'étude The Global State of Information Security Survey 2016 réalisée par le cabinet d'audit et de conseil PwC, en France, le nombre de cyber-attaques recensées a progressé à hauteur de 51% au cours des 12 derniers mois.
Cette explosion est supérieure à la hausse constatée au niveau mondial, le nombre de cyber-attaques visant les entreprises ayant progressé de 38% en 2015.
Cette étude, qui recense la façon dont plus de 10.000 dirigeants dans 127 pays gèrent la cybersécurité dans leurs organisations relève également que ces derniers ont augmenté leur budget pour lutter contre la cyber-criminalité
Au niveau mondial, ces budgets ont augmenté de 24%, renversant la tendance baissière de l'année dernière.

PwC – Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit un budget en hausse de 29% par rapport à l'année dernière

Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit une hausse de 29%, plus élevée que celle constatée au niveau mondial.
Ce chiffre est à comparer avec le niveau estimé des pertes financières liées à des incidents de cybersécurité, soit en moyenne à 3,7 millions d'euros par entreprise en France, soit une augmentation de 28% par rapport à 2014.

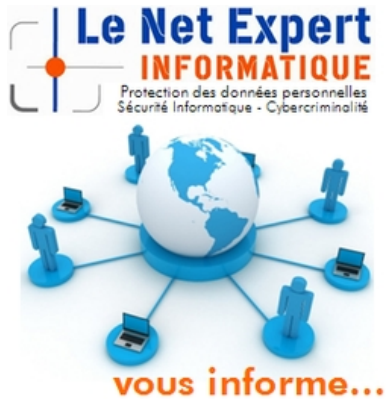
Le piratage de la chaîne TV5 Monde aurait ainsi coûté plus d'une dizaine de millions d'euros.
En France comme dans le monde, la source des menaces reste majoritairement interne aux entreprises. Cependant les sources de cyber-attaques qui ont progressé le plus en 2015 sont, elles, externes aux entreprises.
Le fait saillant tient au fait que la responsabilité des fournisseurs et des prestataires de service actuels est de plus en plus invoquée dans la progression de ces incidents informatiques.

« Ce qui ne peut être protégé, peut être assuré »
Cette responsabilité est en hausse d'environ 32% pour les fournisseurs et de 30% pour les prestataires de services. Cela est dû au fait que les entreprises travaillent de plus en plus en collaboration avec des partenaires commerciaux et industriels externes, ce qui accroît les « portes d'entrée » pour le piratage informatique.
Selon Philippe Trouchaud, associé chez PwC, « Les chiffres indiquent qu'une entreprise française sur 5 pense que ses concurrents sont potentiellement à l'origine de certaines attaques subies en 2015. En effet, ces derniers sont particulièrement attirés par les données de type propriété intellectuelle, les business plans, les données de R&D, etc ».
« Ce qui ne peut pas être protégé peut être assuré », note PwC, qui estime que le marché mondial de la cyberassurance (pour atténuer les effets financiers d'une cyberattaque) va tripler d'ici 2015, à 7,5 milliards de dollars.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://bfmbusiness.bfmtv.com/entreprise/en-france-les-cyber-attaques-sur-les-entreprises-explosent-922703.html
Par F.Bergé

Les entreprises doivent se préparer à une nouvelle génération de cyber-risques | Le Net Expert Informatique



ALes entreprises doivent se préparer à une nouvelle génération de cyber-risques

Les entreprises doivent se préparer à une nouvelle génération de cyber-risques qui progressent rapidement, passant de menaces avérées de violations de données, problèmes de confidentialité et atteintes à la réputation, à l'interruption d'activité et même à des pertes potentielles catastrophiques, en passant par des dommages opérationnels.

Dans un nouveau rapport — A Guide to Cyber Risk : Managing The Impact of Increasing Interconnectivity —, l'assureur spécialisé Allianz Global Corporate & Specialty (AGCS) observe les dernières tendances en matière de cyber-risques et les dangers émergents au niveau mondial. Le cyber-risque est l'une des principales menaces auxquelles font face les entreprises et connaît une croissance rapide. La cybercriminalité à elle seule coûte approximativement 445 milliards de $ par an à l'économie mondiale et les 10 plus grandes économies représentent plus de la moitié de ce montant (3 milliards de $ pour la France).
« Il y a à peine 15 ans, les cyber-attaques étaient assez rudimentaires et généralement l'œuvre de hacktivistes, mais avec l'accroissement de l'interconnectivité, de la mondialisation et de la commercialisation de la cybercriminalité, la fréquence et la gravité des cyber-attaques ont pris une ampleur considérable », déclare Chris Fischer Hirs, PDG d'AGCS. « La cyber-assurance ne remplace pas une sécurité informatique solide, mais elle crée une seconde ligne de défense qui limite les incidents. AGCS observe une augmentation de la demande pour ces services, et nous nous engageons à collaborer avec nos clients afin de mieux comprendre l'exposition croissante aux cyber-risques et d'y faire face. »

Des réglementations plus strictes et de nouveaux cyber-dangers

Une prise de conscience croissante des expositions aux cyber-risques ainsi qu'une adaptation de la réglementation vont propulser la croissance future de la cyber-assurance. Avec moins de 10 % des entreprises qui achètent actuellement des cyber-polices spécifiques, AGCS prévoit une augmentation des primes de cyber-assurance à l'échelle mondiale de 2 milliards de $ par an aujourd'hui à plus de 20 milliards de $ au cours de la prochaine décennie, soit un taux de croissance annuel de plus de 20 %.
« Aux États-Unis, la croissance a déjà commencé, portée par des règles relatives à la protection des données qui attirent l'attention sur le problème. Dans le reste du monde, de nouvelles dispositions législatives et des niveaux de responsabilité plus élevés seront des moteurs de croissance », affirme Nigel Pearson, responsable mondial de la cyber-assurance chez AGCS. « La tendance générale tend à opter pour une protection des données plus strictes et elle est soutenue par la menace d'amendes importantes en cas d'infraction. » Hong Kong, Singapour et l'Australie, par exemple, travaillent sur de nouvelles lois ou en appliquent déjà. Même si l'Union européenne ne parvient pas à se mettre d'accord sur ses règles paneuropéennes de protection des données, on peut s'attendre à des directives plus strictes à l'échelle de chaque pays.
Auparavant, l'attention se focalisait largement sur la menace de violation de données d'entreprise et d'atteinte à la vie privée, mais la nouvelle génération de cyber-risques est plus complexe : les menaces futures porteront sur le vol de propriété intellectuelle, la cyber-extorsion et l'impact de l'interruption d'activité après une cyber-attaque, ou sur une défaillance opérationnelle ou technique — un risque qui est souvent sous-estimé. « La prise de conscience des risques d'interruption d'activité et de l'assurance relative aux cyber-risques et à la technologie ne cesse de croître. Dans les cinq à dix prochaines années, l'interruption d'activité sera perçue comme un risque majeur et un élément principal du paysage des cyber-assurances », déclare Georgi Pachov, expert cyber dans l'équipe de souscription mondiale Dommages aux Biens d'AGCS. Dans le contexte des cyber-risques et des risques informatiques, la couverture interruption d'activité peut être très étendue, incluant les systèmes informatiques d'entreprise, mais aussi les systèmes de contrôle industriel (SCI) utilisés par des entreprises du secteur de l'énergie, ou encore les robots utilisés dans la production.

La connectivité engendre le risque

L'interconnectivité accrue des appareils que nous utilisons au quotidien et la dépendance croissante à la technologie et aux données en temps réel au niveau personnel comme à l'échelle de l'entreprise, connue sous le nom d'« Internet des objets », créent d'autres vulnérabilités. Certaines estimations suggèrent qu'un billion d'appareils pourraient être connectés d'ici 2020 et 50 milliards de machines pourraient échanger des données quotidiennement. Les SCI sont un autre sujet de préoccupation étant donné que nombre de ces systèmes qui sont toujours utilisés aujourd'hui ont été conçus avant que la cyber-sécurité devienne un problème prioritaire. Une attaque contre un SCI pourrait donner lieu à des dommages matériels comme un incendie ou une explosion, ainsi qu'à une interruption d'activité.

Evénements catastrophiques

Alors que des violations de données très importantes ont déjà eu lieu, la perspective d'une perte catastrophique est devenue plus probable, mais il est difficile de prédire ce qu'elle impliquera exactement. Les scénarios comprennent une attaque réussie contre l'infrastructure de base d'Internet, une violation grave des données ou une panne de réseau chez un fournisseur de cloud, alors qu'une cyber-attaque importante impliquant une entreprise d'énergie ou de services publics pourrait se traduire par une interruption significative des services, des dommages matériels ou même des pertes humaines à l'avenir.

Couverture autonome

D'après Allianz, la portée de la cyber-assurance doit également évoluer en vue de fournir une couverture plus étendue et plus approfondie, prenant en charge l'interruption d'activité et comblant les lacunes entre la couverture traditionnelle et les cyber-polices. Alors que les exclusions des cyber-risques dans les polices IARD vont vraisemblablement devenir monnaie courante, la cyber-assurance autonome va continuer d'évoluer pour devenir la source principale de couverture complète. On observe un intérêt croissant dans les secteurs des télécommunications, de la distribution, de l'énergie, des services publics et du transport, ainsi que de la part des institutions financières.

La formation — en termes de compréhension de l'exposition de l'entreprise comme de connaissances en souscription — doit s'améliorer pour permettre aux assureurs de répondre à une demande croissante. De plus, comme pour tout autre risque émergent, les assureurs doivent en outre faire face à des défis concernant la tarification, les libellés des polices non testés, la modélisation et l'accumulation des risques.

Réponse aux cyber-risques

Le rapport d'AGCS expose les démarches que les entreprises peuvent entreprendre pour couvrir les cyber-risques. L'assurance ne peut être qu'une partie de la solution, avec une approche globale de la gestion des risques en guise de fondement de la cyberdéfense. « Le fait de contracter une cyber-assurance ne signifie pas que vous pouvez ignorer la sécurité informatique. Les aspects technologiques, opérationnels et assurantiels de la gestion des risques vont de pair », explique Jens Krickhahn, expert Cyber & Fidelity chez AGCS Central & Eastern Europe. La gestion des cyber-risques est trop complexe pour être l'apanage d'un seul individu ou département, de sorte qu'AGCS recommande la constitution d'un groupe de réflexion pour combattre les risques, au sein duquel différentes parties prenantes dans toute l'entreprise collaboreraient pour partager leurs connaissances.

De cette manière, différentes perspectives sont remises en question et d'autres scénarios sont pris en considération : ceux-ci peuvent par exemple inclure le risque découlant des développements de l'entreprise comme les fusions et acquisitions, ou de l'utilisation de services externalisés ou d'un cloud. De plus, la contribution intersociétés est essentielle pour identifier les actifs clés en matière de risque et, surtout, pour développer et tester des plans d'action solides en cas de crise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.globalsecuritymag.fr/Allianz-Global-Corporate-Specialty,20150909,55621.html

---

La propriété intellectuelle à l'épreuve de l'impression 3D. Par Augustin Deschamps, Juriste. | Le Net Expert Informatique

La propriété intellectuelle à l'épreuve de l'impression 3D

Le Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA) a introduit en juillet 2015 une nouvelle commission dédiée à l'impression en trois dimensions. Présidé par le conseiller d'Etat Olivier Japiot, ce nouveau cercle de travail aura pour mission de rédiger un rapport pour le mois de juin 2016 sur les nouveaux enjeux de la propriété intellectuelle soulevés par la démocratisation de l'imprimante 3D.

L'impression 3D est donc en passe de devenir personnelle : il est aujourd'hui possible d'imaginer, dessiner, modéliser puis fabriquer un objet quelconque. De manière plus troublante, il sera bientôt concevable de scanner n'importe quel objet acheté dans le commerce, pour le reproduire à l'infini. Par exemple, la copie d'un fauteuil dessiné par Philippe Starck est aujourd'hui techniquement possible. Sans aller jusqu'à parler d'une « quatrième révolution industrielle », il est certain qu'un changement de paradigme s'opère peu à peu, ce qui soulève des enjeux évidents en matière de propriété intellectuelle.
Car même si beaucoup d'acteurs de ce nouveau marché se positionnent en faveur d'une libre diffusion des contenus imprimables, en open source ou via les licences Creative Commons, le développement de l'impression 3D provoque déjà de nombreuses atteintes aux droits de propriété intellectuelle des artistes, inventeurs et de tous les auteurs d'oeuvres de l'esprit.

L'ensemble des composants de la propriété intellectuelle sont concernés par l'impression en trois dimensions

Le bouleversement lié à l'apparition du MP3 sur le marché de la musique ne touchait que le droit d'auteur, tandis que le l'impression 3D nécessite d'envisager l'ensemble de la propriété littéraire et artistique, ainsi que la propriété industrielle. L'enjeu réside autour de la contrefaçon des biens protégés : celle-ci sera caractérisée en fonction de l'usage affecté à l'objet imprimé.

De manière générale, l'usage collectif, public, ou même commercial d'un tel objet permettra de qualifier un acte de contrefaçon. Tout individu imprimant un objet portant atteinte au droit d'auteur, aux dessins et modèles ou même à un brevet sera qualifié de contrefacteur. Concernant l'utilisation illicite d'une marque déposée, la jurisprudence impose un usage dans la vie des affaires pour reconnaître une contrefaçon.

Dans le cas contraire, un usage strictement privé de l'objet imprimé permettra d'échapper aux sanctions rattachées à la contrefaçon. Plus spécifiquement, concernant le droit d'auteur, les objets imprimés en 3D bénéficient de l'exception de copie privée. Ce régime spécifique autorise « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ». Actuellement, la copie privée s'applique majoritairement aux contenus audiovisuels et musicaux, ce qui pose la question de la congruence d'un tel régime avec l'impression 3D.

L'exception de copie privée applicable en l'état ?

Le Code de la propriété intellectuelle dispose en effet que les exceptions de copie privée « ne peuvent porter atteinte à l'exploitation normale de l'oeuvre ni causer un préjudice injustifié aux intérêts légitimes de l'auteur. » C'est sur ce fondement qu'un individu a été débouté par le juge de sa demande de faire lever les mesures techniques de protection (MTP) d'un DVD car il souhaitait en offrir une copie à ses parents. Il est dès lors possible de penser que les MTP, qui empêchent efficacement l'atteinte aux droits de propriété intellectuelle rattachés à un film DVD, pourraient s'appliquer de manière analogue aux fichiers 3D en limitant le nombre d'impressions. Cette protection semble d'autant plus souhaitable que l'impression 3D décuple les potentiels préjudices des titulaires de droits d'auteur. Le scan et l'impression 3D d'une douzaine de chaises design à partir d'une permettront une économie substantielle pour le copiste, et par conséquent un manque à gagner démultiplié pour le propriétaire des droits sur le design industriel du meuble reproduit. L'exception de copie privée appliquée à l'impression 3D voit dès lors son efficacité limitée par la possible multitude des copies. Bien sûr, il est possible de copier un album de musique à l'infini, mais il ne viendrait probablement pas à l'esprit du consommateur d'en acheter plusieurs pour en avoir un dans sa voiture, un chez lui et un au bureau. Le manque à gagner est réel pour les propriétaires des droits de l'album, mais moindre que pour un bien mobilier.

De surcroît, le Sénat a ce mois-ci rejeté l'idée d'une redevance copie privée pour les imprimantes 3D, telle qu'elle existe déjà pour les supports de stockage (CD vierges, clés USB…) pour compenser le préjudice des artistes. L'argument principal des parlementaires a été d'affirmer que la copie 3D est une contrefaçon, donc illicite, et qu'une redevance ne peut s'appliquer à une activité illégale. Le Ministre de l'économie a ajouté qu'il n'était pas souhaitable de freiner le développement des acteurs français du domaine de l'impression tridimensionnelle.

En revanche, lorsqu'un objet sera imprimé après avoir été dessiné par le consommateur lui-même, ou téléchargé en open source, il ne sera pas possible de caractériser un acte de contrefaçon. Une telle utilisation de l'imprimante 3D ne sera qu'une extension du « do it yourself » (DIY) qui est de plus en plus en vogue. Certains professionnels l'ont compris, à l'image de l'enseigne Castorama qui a pour projet de créer une plateforme en ligne dédiée aux fichiers 3D permettant l'impression de pièces détaché d'électroménager ou de bricolage directement chez soi. Ce nouveau service créera une concurrence sévère vis-à-vis des artisans et revendeurs de produits électroménagers.

De nécessaires solutions pour protéger les titulaires de droits de propriété intellectuelle sans entraver l'avancement technologique

Les auteurs ont déjà la possibilité de procéder à un dépôt en ligne de leurs fichiers 3D auprès d'une société de gestion de droit, ou directement chez un notaire ou un huissier qui rédigera un procès verbal qui justifiera de la date de création de l'oeuvre. Cette démarche a pour utilité de prouver l'antériorité de la création, mais ne prémunit pas l'auteur contre les risques de contrefaçon. À cette fin, il pourrait être efficace de développer des services de « streaming 3D », ne permettant l'impression d'un fichier qu'une seule fois, grâce à des mesures techniques de protection. Une telle restriction pourrait par ailleurs s'accompagner de l'impossibilité de modifier l'oeuvre imprimée, faisant ainsi respecter son intégrité.

Une autre option consisterait à implanter dans toutes les imprimantes 3D un système de vérification de la licéité de l'impression. Connectée à internet, l'imprimante pourrait rechercher l'existence de droits de propriété intellectuelle sur l'objet, ainsi que l'absence de caractère dangereux. En effet, les pièces détachées d'armes à feu sont facilement reproductibles, ce qui a pour principale conséquence l'absence de numéro de série et donc l'impossibilité de toute traçabilité. Il est cependant nécessaire de noter qu'une telle surveillance constituerait une immixtion manifeste dans la vie privée des utilisateurs, ajoutant une nouvelle dimension au problème de l'exploitation des données personnelles.

Aujourd'hui, la distance entre l'objet original et la copie imprimée en 3D demeure importante, de telle sorte que la confusion n'est pas possible. Il est concevable de reproduire une forme, mais pas encore les mécanismes intérieurs, qui relèvent pour certain de la « 4D ». De nombreuses contraintes techniques demeurent mais la rapidité des progrès accomplis permet d'entrevoir l'étendue des enjeux juridiques de demain, et il ne fait aucun doute que ce sujet, qui alimente beaucoup de fantasmes, sera l'objet de débats passionnés.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.village-justice.com/articles/propriete-intellectuelle-epreuve,20280.html
Par Augustin Deschamps juriste chez LegaLife

Fuite d'une ébauche du projet de loi numérique d'Axelle Lemaire | Le Net Expert Informatique

Fuite d'une ébauche du projet de loi numérique d'Axelle Lemaire

Si la version « bêta » du projet de loi numérique n'a toujours pas été publiée (et ce alors qu'Axelle Lemaire avait indiqué que ce serait le cas « avant la fin du mois de juin »), Contexte vient de publier une version de travail du texte élaboré sous la houlette de Bercy. Ce document non définitif nous permet d'en savoir davantage sur la façon dont le gouvernement pourrait concrétiser ses ambitions.

L'ébauche diffusée par nos confrères date de début juillet, avant que la piste d'une seconde loi relative au numérique – et portée cette fois par le ministre de l'Économie, Emmanuel Macron – ne soit confirmée par le gouvernement. « Selon nos informations, le texte a évolué depuis, et n'est toujours pas complètement stabilisé. Les réunions interministérielles de validation n'ont pas encore commencé » insiste d'ailleurs le journaliste Samuel Le Goff, pour bien faire comprendre que beaucoup de choses risquent de bouger d'ici à la publication de l'avant-projet de loi censé être soumis aux commentaires des internautes cet été…
Cette version de travail, longue d'une trentaine de pages, contient malgré tout plus de 80 articles. On y retrouve les principales mesures distillées au fil du temps par la secrétaire d'État au Numérique, Axelle Lemaire, ou même par Manuel Valls. Tour d'horizon.

Open Data
Ouverture par défaut des données publiques détenues par l'administration. L'État, les collectivités territoriales et les personnes chargées d'une mission de service public seraient tenus de diffuser automatiquement leurs documents administratifs communicables au sens de la loi CADA, dès lors que ceux-ci existent au format électronique. Aucune référence au format de mise en ligne de ces documents ne figure cependant dans cette version de travail. L'entrée en vigueur de ces dispositions est par ailleurs progressive : dans les six mois pour des « bases de données de référence définies par un arrêté du Premier ministre », puis deux ans pour les documents administratifs reçus ou produits après la promulgation de la loi, et enfin cinq ans pour l'ensemble des documents.
Principe de gratuité. La réutilisation d'informations publiques deviendrait gratuite, également par défaut. Des redevances pourront toujours être réclamées par des administrations, à condition toutefois que « le coût de la reproduction ou de la numérisation des documents administratifs concernés ou l'anonymisation des informations qu'ils contiennent représente une part significative de leurs ressources ». Un registre public serait spécialement créé afin de rassembler toutes les informations relatives à ces différentes redevances.
Création d'un « service public de la donnée ». Sous la houlette de l'Administrateur général des données, dont les missions sont gravées dans le marbre, ce service public de la donnée aurait pour objectif de faciliter la circulation de données entre administrations. Pour la première fois, il est prévu que des décrets puissent exiger « la transmission de données à l'administrateur général des données, lorsque cette transmission est nécessaire à la constitution ou à la mise à jour des données de référence ».
Statut pour les « données d'intérêt général ». Les délégataires de services publics ou les organisations recevant des subventions de plus d'un million d'euros pourraient être contraintes de mettre en Open Data certaines données produites dans le cadre de leur mission, financée sur deniers publics. L'ouverture de données purement privées (environnement, énergie…) pourrait également être exigée par les pouvoirs publics, dès lors qu'il y aurait un « motif d'intérêt général, tenant notamment à leur contribution déterminante à la mise en œuvre d'une politique publique, à la recherche [publique] ou au développement d'activités économiques nouvelles ». Ces dispositions risquent toutefois d'évoluer suite aux travaux menés par la mission Cytermann (voir notre article).

Ouverture du code source des logiciels développés par l'État
Les « codes source des logiciels » figureraient expressément parmi la liste des informations publiques considérées communicables au sens de la loi CADA.

Protection des données personnelles
Plusieurs articles ont été rédigés afin que chaque utilisateur d'un service en ligne puisse obtenir la copie des données collectées à son égard, dans « un format électronique ouvert et permettant une réutilisation effective de ces données ». Des dispositions spécifiques aux emails ont également été insérées.

Renforcement des missions la CNIL
L'institution pourrait être « obligatoirement consultée sur tout projet de loi ou de décret comportant des dispositions relatives à la protection des données à caractère personnel ou au traitement de telles données ». Elle serait même autorisée à « prendre l'initiative de donner un avis » sur toute question relative la protection des données personnelles, notamment en direction du législateur.

Plus de pouvoirs pour la CNIL
Les sanctions prononcées par la Commission pourraient devenir bien plus dissuasives pour les géants du numérique : jusqu'à 3 millions d'euros ou, pour les entreprises, 5 % de leur « chiffre d'affaires annuel mondial ». On serait ainsi bien loin des 300 000 euros maximums prévus actuellement (et uniquement en cas de manquements répétés…). En cas d'urgence, la CNIL pourrait d'autre part ordonner au responsable d'un traitement de respecter la loi Informatique et Libertés dans un délai de 24 heures, contre 5 jours actuellement.

Action collective pour les litiges relatifs aux données personnelles
Sur le modèle des nouvelles actions de groupe, des internautes pourraient saisir les juridictions civiles par le biais notamment d'associations de consommateurs, et ce « afin d'obtenir la cessation d'une violation » à la loi Informatique et Libertés. Assez curieusement, ce dispositif ne fonctionnerait pas pour les traitements de données personnelles mis en œuvre dans le cadre d'un service public administratif.

Droit à l'oubli pour les mineurs
Le fait qu'une personne ait moins de 18 ans au moment où une donnée la concernant est collectée serait un « motif légitime » justifiant l'arrêt de son traitement, « sauf si la personne mineure était une personnalité publique ».

Droit de « mort numérique »
Chaque internaute pourrait laisser des directives concernant le devenir de ses données personnelles, en cas de décès. La personne désignée (ou, à défaut, les héritiers) auraient ensuite le pouvoir de se tourner vers les réseaux sociaux ou autres services en ligne pour obtenir par exemple la suppression des données ou du compte du défunt, etc.

Des pistes très variées
Neutralité du Net. Posant le principe que l'exploitant d'un réseau de communication électronique n'a « ni la connaissance ni le contrôle des informations reçues ou transmises par des tiers », des restrictions ne pourraient être mises en œuvre « que dans le respect des principes de non-discrimination, de proportionnalité, de nécessité et de transparence lorsque le niveau de qualité du service n'est pas garanti ».

Définition positive du domaine public. L'ébauche diffusée par Contexte comprend un article qui reconnaît expressément un « domaine public informationnel », composé premièrement des « informations, données, faits, idées, principes et découvertes, dès lors qu'ils ont fait l'objet d'une divulgation publique » ; deuxièmement des « objets qui ne sont pas couverts par les droits prévus dans le Code de la propriété intellectuelle ou dont la durée de protection légale a expiré » ; et troisièmement des « documents administratifs diffusés publiquement » par l'État, les collectivités territoriales, etc.

De nombreux autres sujets sont abordés, tels que la régulation des jeux d'argent en ligne, le renforcement des pouvoirs de l'ARCEP (le régulateur des télécoms), la loyauté des plateformes, etc. Sauf que certains de ces sujets auront plus vraisemblablement leur place dans l'éventuel projet de loi « Macron II », dont les mesures devraient être davantage tournées vers l'aspect économique. Résultat dans quelques jours, si le gouvernement se décide à publier (enfin) la version « bêta » du projet de loi numérique d'Axelle Lemaire.

Source : http://www.nextinpact.com/news/95876-fuite-d-une-ebauche-projet-loi-numerique-d-axelle-lemaire.htm
Par Xavier Berne

WHOIS : vos informations personnelles bientôt publiques ? | Le Net Expert Informatique

L'ICANN pourrait bientôt modifier le système du WHOIS. Le régulateur propose notamment d'interdire aux propriétaires de sites « à but commercial » de s'enregistrer via proxy, soit de façon anonyme. Le texte ne laisse pas les associations insensibles, qui y voient une menace pour ceux qui s'expriment librement sur leurs sites.

WHOIS est souvent décrit comme l'annuaire d'Internet. Lors de l'enregistrement d'un nom de domaine, un internaute doit renseigner diverses informations personnelles, de son état civil à son numéro de téléphone en passant par son adresse de domicile. Ces informations alimentent les bases de données des registres de noms de domaine, et sont consultables via l'outil WHOIS.
Pour des questions évidentes de protection de la vie privée et de confidentialité, les données fournies par le propriétaire d'un nom de domaine ne sont pas accessibles au public. Les registres de renseignement proposent fréquemment en option la possibilité de s'enregistrer via proxy. Les seules tierces personnes alors en mesure d'accéder aux bases de données non anonymisées sont celles détenant une autorisation légale, tel qu'un mandat judiciaire.
Mais cette situation connaîtrait ses derniers jours. L'ICANN prévoit en effet de modifier le système en profondeur. Le régulateur étudie actuellement un projet, lequel envisage notamment que les noms de domaine « utilisés dans un but commercial soient inéligibles à l'enregistrement proxy/privacy ». En d'autres termes, les propriétaires de sites contenant un quelconque élément transactionnel ne pourront plus s'enregistrer de façon anonyme : leurs informations personnelles devront être publiques.

L'anonymat, garant de la liberté d'expression
Alors que l'ICANN doit se prononcer le 7 juillet sur ce texte, l'Electronic Frontier Foundation appelle les internautes à s'y opposer. Selon l'EFF, le terme « but commercial » englobe un grand nombre de sites, et la vie privée de leurs propriétaires, des personnes physiques, seraient menacée. L'association prend pour exemple TG Storytime, un site destiné aux auteurs transgenres et hébergés par Joe Six-Pack, lui-même transgenre. Si l'ICANN devait modifier la régulation en vigueur, ses adresses, numéros de téléphone et mails seraient alors exposées à la vue de tous, trolls et harceleurs compris.
Le changement a été impulsé par les géants américains du divertissement, signale l'EFF, ce que l'ICANN ne cache pas. En effet, à de nombreuses reprises, le régulateur d'Internet écrit que cette proposition vise à faciliter le signalement de sites violant le droit d'auteur (ou toute autre propriété intellectuelle). Pour l'EFF, « ces entreprises veulent de nouveaux outils pour découvrir l'identité des propriétaires de sites Web qu'ils veulent accuser de violation de droit d'auteur et contrefaçon de marque, de préférence sans une ordonnance du tribunal ».
« L'avantage limité de cette évolution est manifestement compensé par les risques supplémentaires pour les propriétaires de sites, qui vont souffrir d'un risque plus élevé de harcèlement, d'intimidation et de vol d'identité ».
Il est vrai que, malgré les gardes fous prévus par l'ICANN, la plupart des informations fournies pour l'enregistrement d'un nom de domaine sont sensibles, tant IRL (In Real Life) que dans le monde virtuel. En appelant à s'opposer au texte, l'association entend faire réagir sur un recul de l'anonymat, qui affectera ceux qui portent des opinions impopulaires ou marginales mais aussi les lanceurs d'alerte et tous ceux susceptibles de dénoncer « la criminalité et la corruption ».

Source : http://www.linformaticien.com/actualites/id/37199/whois-vos-informations-personnelles-bientot-publiques.aspx
Par Guillaume Périssat

Votre entreprise est-elle assurée contre les pirates informatiques ? | Le Net Expert Informatique

	Cyberattaques: votre entreprise est-elle assurée contre les pirates ?

Pertes de données, poursuites judiciaires, systèmes informatiques endommagés… les cyberattaques représentent une nouvelle gamme de risques auxquels les entreprises petites et grandes sont confrontées. Sentant la bonne affaire, certains assureurs offrent maintenant une protection contre ces écueils. En quoi consiste une telle assurance ? Est-elle devenue incontournable ?

Évaluer les risques

Inutile de parler d'assurance si on ne connaît pas d'abord le risque auquel on est exposé. Celui d'être victime d'une cyberattaque ne se mesure pas tant selon la taille de l'entreprise que par rapport au type d'information que l'on y traite. Ce n'est donc pas seulement le souci des grandes boîtes. L'étude «Internet Security Threat Report 2014» du concepteur d'antivirus Symantec révèle d'ailleurs que 61 % des hameçonnages ciblés ont visé des PME en 2013, comparativement à 50 % un an plus tôt.

Or, des études récentes de Cisco montrent qu'un peu plus de la moitié des entreprises canadiennes n'ont pas encore mis en place un plan en matière de sécurité informatique. «C'est primordial pour déterminer les types de renseignements à protéger, les moyens de les stocker, les personnes qui y ont accès, l'équipement, etc.», précise Maya Raic, présidente-directrice générale de la Chambre de l'assurance de dommages.

Stockez-vous sur vos serveurs une base de données contenant le numéro d'assurance sociale de médecins spécialistes ? Ou un simple catalogue de vos produits ? Les données ont un degré de sensibilité variable. Cela dit, plus vous traitez de l'information de tiers ou de la propriété intellectuelle, plus vous avez de risques de poursuites en cas de brèche de sécurité.

« 117 339: c'est le nombre de cyberattaques commises chaque jour dans le monde, d'après une récente enquête de PwC. Et ce ne sont là que celles dont les entreprises sont conscientes, puisque près des 3/4 des attaques ne sont pas décelées. »

Des polices sur mesure

«On compte actuellement une dizaine d'assureurs au Canada qui protègent les entreprises contre les cyberrisques», soutient Maya Raic.

Comme on n'en est qu'aux balbutiements de ce type d'assurance, les clauses varient d'un assureur à l'autre. «On traite encore les clients au cas par cas, donc ceux-ci peuvent négocier les termes», mentionne Jean-François De Rico, associé au cabinet d'avocats Langlois Kronström Desjardins.

Les polices peuvent couvrir la responsabilité liée aux pertes de données (les recours collectifs potentiels, les atteintes à la réputation commerciale ou les frais liés au redémarrage des systèmes), la gestion de crise, l'interruption des affaires, la cyberextorsion, etc.

Quant aux exclusions standards, ces polices n'en comportent pas vraiment, contrairement aux autres types d'assurance qui excluent d'emblée certains risques. Ce que vous pourriez voir toutefois, c'est une clause qui délimite le cadre de l'assurance. «Par exemple, la responsabilité civile des dirigeants et des administrateurs n'est pas couverte par la cyberassurance, puisque cette protection existe déjà dans une autre police d'assurance sans lien avec le cybercrime», illustre Alexis Héroux, courtier en assurance de dommages chez Marsh Canada.

« Installer les mises à jour dans les 48h où elles sont disponibles par les fournisseurs d'antivirus réduit les risques de cyberattaques de 85%. »

C'est combien ?

Les limites de couverture varient énormément selon les compagnies d'assurance et peuvent aller de 500 000 dollars à 20 millions de dollars. Si plusieurs assureurs se réunissent, la limite peut même atteindre 250 millions de dollars.

On devine que le coût des primes varie tout autant, selon la limite choisie et l'ensemble des facteurs qui peuvent influencer le risque : le type et la quantité de données utilisées et recueillies par l'entreprise, le système de gestion en place, etc. Les PME dont les besoins de protection sont moindres pourraient réussir à obtenir une prime annuelle minimale de 1 500 dollars, mais c'est en général beaucoup plus coûteux. Retenez surtout que tout se négocie, selon votre budget.

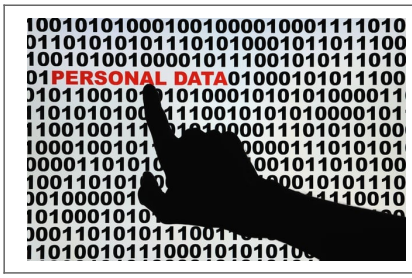
« 201$: c'est le prix que coûte en moyenne chaque donnée de tiers sensible et confidentielle qui a été volée. »

Cela dit, comme pour les autres types d'assurance, les cyberrisques ne reposent jamais entièrement sur les épaules des assureurs. L'entreprise a sa part de responsabilité. Aussi, plus on a une infrastructure de sécurité sophistiquée et bien gérée, plus on réduit le risque, et donc le coût de la prime (voire la nécessité d'une protection d'assurance).

Cependant, quand on sait que même des spécialistes comme Symantec ont déjà été victimes d'une cyberattaque, il vaut mieux, parfois, investir un certain montant en assurance pour couvrir ces nouveaux aléas.

Source : http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-votre-entreprise-est-elle-assuree-contre-les-pirates-/579164

La protection des données personnelles, un marché juteux en Suisse



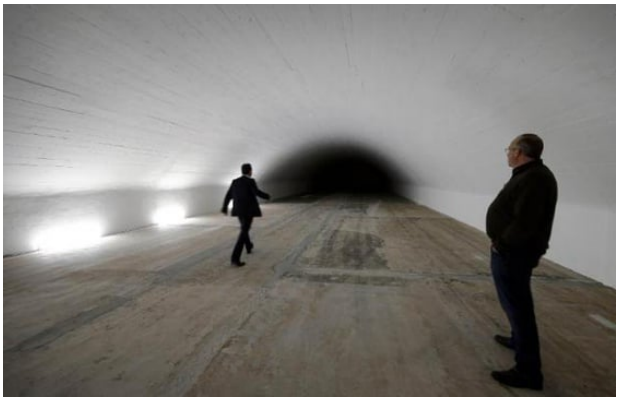
La protection des données personnelles, un marché juteux en Suisse

«Données 100% stockées en Suisse.» De plus en plus d'entreprises mettent en avant sur leur site ce petit macaron aux couleurs de la Confédération helvétique, qui pourrait faire de la protection des données personnelles une nouvelle source de prospérité du pays. «Les données sont le nouvel eldorado de la Suisse. C'est un vrai boom», se réjouit ainsi Franz Grüter, directeur général de Green.ch, l'une des principales entreprises suisses spécialisées dans le stockage de données personnelles, qui connaît une croissance annuelle de 30%.

Les scandales d'espionnage généralisé à la suite des révélations de l'ex-conseiller de l'Agence nationale de sécurité (NSA) américaine Edward Snowden ont permis une prise de conscience accrue, notamment du côté des entreprises, sur la nécessité de protéger ses données personnelles et dont la Suisse compte bien tirer parti. «Les clients ont besoin de confiance, de discrétion, de fiabilité et de stabilité. Or ce sont les caractéristiques de ce pays depuis toujours», ajoute Franz Grüter, selon qui plus d'un milliard de francs (1 milliard d'euros) ont été investis ces cinq dernières années dans des centres de données informatiques du pays.

De la Silicon Valley à Zurich

«Un Etat offrant un niveau de protection élevé à ses entreprises leur offre également des avantages économiques non négligeables», estime pour sa part Jean-Philippe Walter, adjoint au Préposé fédéral à la Protection des données et à la transparence. Et avec 61 centres de données sur les 1.151 situés dans l'Union européenne (selon le site datacentermap), la Confédération se classe aujourd'hui à la cinquième place européenne. Le contexte juridique est d'ailleurs très favorable à la Suisse : sa loi sur la protection des données, l'une des plus restrictives au monde, empêche toute administration d'avoir accès à des informations personnelles sans l'autorisation d'un juge.



La Suisse utilise les anciens bunkers de la guerre froide comme coffre-fort numérique.
Ici, celui situé près d'Attinghausen, repère de la société Deltalis dont le code GPS est tenu secret.

En conséquence, certaines entreprises étrangères n'hésitent pas à se relocaliser en Suisse. C'est le cas de Multiven, l'un des leaders mondiaux de la maintenance des réseaux Internet, qui a quitté la Silicon Valley californienne pour Zurich en 2009. «Nous prévoyons un avenir dans lequel les individus, les entreprises et les organisations du monde entier chercheront à stocker leurs actifs numériques (propriété intellectuelle, inventions, secrets commerciaux…) en Suisse pour transformer le pays de sanctuaire d'actifs physiques (espèces, or, art) en sanctuaire d'actifs numériques, estime sa présidente, Deka Yussuf pour qui la majorité des actifs qui seront enregistrés en Suisse seront numériques d'ici les 25 prochaines années.

Se positionner avant la nouvelle législation européenne

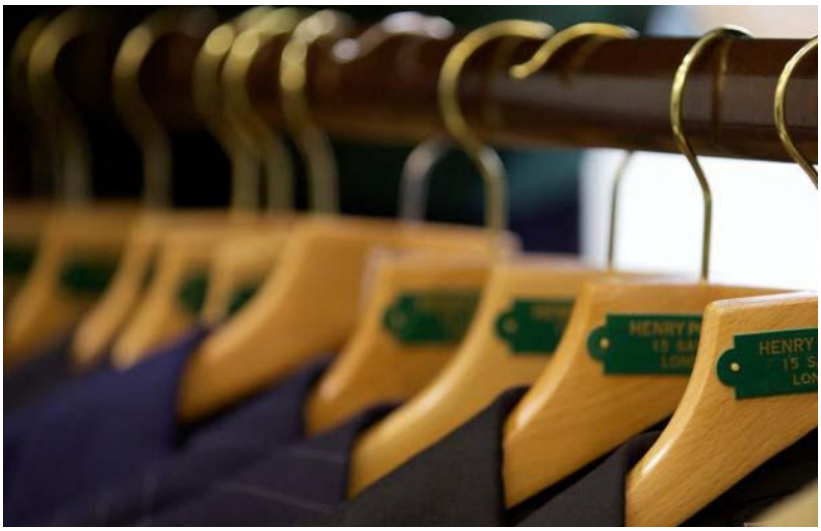
Ainsi, il s'avérerait que les récentes observations faites par le Premier ministre britannique David Cameron et le président américain Barack Obama souhaitant interdire le chiffrement, inaccessible pour leur gouvernement, seraient impensables en Suisse.

Un pays qui suit désormais de près la réforme du régime européen de protection des données personnelles, qui devrait voir le jour d'ici quelques semaines. Ce nouveau cadre renforcerait la législation sur le traitement des données personnelles des citoyens européens par les entreprises et ce, indépendamment de leur localisation géographique et de leur taille. La problématique du stockage des données deviendra alors centrale en Europe; à la Suisse de se positionner en conséquence.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.20minutes.fr/monde/1524251-20150123-suisse-protection-donnees-personnelles-marche-juteux
Illustration : Sébastien SALOM

Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes – 20minutes.fr



Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes

Près de la moitié (49%) des entreprises de distribution et de biens de consommation au niveau mondial déclarent avoir été victimes de fraudes au cours des deux dernières années, selon une étude de PwC diffusée lundi.

«Ce chiffre ne cesse d'augmenter depuis 2009 (+12 points)», note le cabinet de conseil, qui a interrogé 5.128 dirigeants d'entreprises, dont 383 du secteur de la distribution et des biens de consommation, issus de 99 pays. La fraude la plus largement commise dans le secteur est le détournement d'actifs (76%), ce qui inclut «le vol, les décaissements frauduleux et l'appropriation illicite de matériel».

Risques liés à la cybercriminalité

La fraude aux achats arrive en deuxième position, beaucoup de répondants évoquant notamment des infractions liées à la sélection des fournisseurs (59%) ou bien aux contrats/accords de maintenance conclus avec ces derniers (39%).
Si la corruption n'est pas la fraude la plus constatée (25%), 56% des dirigeants interrogés la considèrent comme le risque le plus élevé pour une entreprise opérant à l'international.
Beaucoup de dirigeants évoquent également les risques grandissants liés à la cybercriminalité: un sur cinq déclare en avoir été déjà victime, et 27% pensent que leur entreprise y sera confrontée dans les deux années à venir.

Risque de renvoi ou de poursuites judiciaires

La perte de propriété intellectuelle (contrefaçon, vols de données clients…) fait également partie de leurs préoccupations pour l'avenir: seuls 7% en ont déjà fait l'expérience, mais 21% estiment qu'ils y seront confrontés d'ici deux ans.
L'étude montre que dans plus de deux tiers des cas (67%), les auteurs de ces infractions sont des collaborateurs internes aux entreprises. Ce taux est supérieur dans les secteurs de la distribution/biens de consommation, aux taux constatés sur l'ensemble des secteurs (56%).
«Les auteurs de ces faits occupent, pour la plupart, des postes de cadres intermédiaires et sont sévèrement punis lorsqu'ils sont démasqués: les entreprises pratiquent majoritairement le renvoi; elles se lancent parfois dans des poursuites civiles ou recourent aux autorités judiciaires», indique PwC.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.20minutes.fr/societe/1515087-20150112-vols-cybercriminalite-contrefacons-pres-50-entreprises-victimes-fraudes

---

Live streaming illégal : un coût considérable pour l'économie mondiale

Live streaming illégal : un coût considérable pour l'économie mondiale

Une étude du Center for Strategic and Internationals Studies (CSIS) faisait grand bruit lors de sa sortie, en juin dernier. Elle évaluait à 445 milliards de dollars, soit 327 milliards d'euros, le coût global de la cybercriminalité sur l'économie mondiale. S'il semble compliqué de lutter contre ce fléau sans visage, la limitation de certains comportements à risque permettrait de réduire substantiellement la note pour les industries du secteur, mais aussi et surtout pour les internautes. Ainsi en va-t-il du live streaming illégal, plébiscité mais toxique.

Radiographie de la cybercriminalité mondiale

Sans surprise, les pays les plus exposés aux méfaits des cybercriminels sont les grandes puissances. A eux seuls, Etats-Unis, Chine et Allemagne concentrent 200 milliards de pertes dues à des piratages en tout genre, même si essentiellement par vol de propriété intellectuelle.

L'importance des dégâts commis par les hackers est inversement proportionnelle au nombre d'entre eux capables de conceptualiser des programmes permettant d'exploiter des failles logicielles connues (exploits). Selon le Centre de lutte contre la Cybercriminalité d'Europol, seule une centaine de personnes serait responsable de la cybercriminalité dans le monde. Autrement dit, si d'innombrables réseaux cybercriminels s'approprient les kits d'exploits et malwares créés par d'autres, ils ne sont qu'une poignée à pouvoir être considérés comme les cerveaux du hacking international.

Europol précise que ces kits et malwares sont à ce point élaborés qu'ils peuvent facilement être adaptés aux cibles spécifiques des cybercriminels. Des cibles qui sont souvent des entreprises dont les solutions de sécurité laissent à désirer, mais aussi des particuliers, notamment via leur utilisation du live-streaming illégal, véritables supermarchés pour les hackers, qui n'ont qu'à se pencher pour se servir.

Le live streaming illégal, tête de pont de la cybercriminalité mondiale

Début octobre, l'Association of Internet Security Professionals (AISP) se fendait d'un rapport alarmant. Intitulé « Illegal Streaming and Cyber Security Risks : a dangerous status quo ? » il montrait que 500 millions d'ordinateurs étaient infectés dans le monde, soit une infection toutes les 18 secondes.

Concernant les sites de live streaming illégaux, type retransmission de matchs de sport, le rapport de l'AISP se fait très précis. Selon lui, 80 % de ces plateformes hébergeraient des malwares, visant à subtiliser des données confidentielles aux personnes les fréquentant. Avec pour but, in fine, de bombarder leurs boites mails de spams, de subtiliser leurs codes bancaires ou encore d'usurper leur identité.

67 milliards de dollars sont dépensés par an en achat de services de sécurité sur Internet. Cette somme pourrait être considérablement réduite si les internautes prenaient conscience des risques encourus en surfant, par exemple, sur des sites de live streaming illégaux.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.actu-economie.com/2014/12/18/live-streaming-illegal-cout-considerable-leconomie-mondiale/
Par Christophe Fourrier