Directive européenne sur la sécurité des réseaux et des systèmes d’information

	Directive européenne sur la sécurité des réseaux et des systèmes d’information

Les entreprises qui fournissent des services essentiels, par exemple l'énergie, les transports, les services bancaires et de santé, ou numériques, tels que les moteurs de recherche et les services d'informatique en nuage, devront améliorer leur capacité à résister à des cyber-attaques, selon les premières règles de cybersécurité à l'échelle européenne, approuvées par les députés mercredi.

L'établissement de normes de cybersécurité communes et renforcer la coopération entre les pays de l'Union aidera les entreprises à se protéger elles-mêmes, et aussi à prévenir les attaques contre les infrastructures interconnectées des pays européens, estiment les députés.

« Des incidents de cybersécurité possède très souvent un aspect transfrontalier et concernent donc plus d'un État membre de l'Union européenne. Une protection fragmentaire de la cybersécurité nous rend tous vulnérables et pose un risque de sécurité important pour l'Europe dans son ensemble. Cette directive établira un niveau commun de sécurité de réseau et d'information et renforcera la coopération entre les États membres. Cela contribuera à prévenir à l'avenir les cyberattaques sur les infrastructures interconnectées européennes importantes », a déclaré le rapporteur du Parlement Andreas Schwab (PPE, DE).

La directive européenne sur la sécurité des réseaux et des systèmes d'information « est également l'un des premiers cadres législatifs qui s'applique aux plates-formes. En phase avec la stratégie du marché unique numérique, elle établit des exigences harmonisées pour les plates-formes et veille à ce qu'elles puissent observer des règles similaires quel que soit l'endroit de l'Union européenne où elles opèrent. C'est un énorme succès et une première étape importante vers l'établissement d'un cadre réglementaire global pour les plates-formes dans l'Union », a-t-il ajouté.

Les pays de l'UE devront lister les entreprises de « services essentiels »

La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les « opérateurs de services essentiels » dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable. Les États membres de l'UE devront identifier les entités dans ces domaines en utilisant des critères spécifiques, par exemple si le service est essentiel pour la société et l'économie, et si un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

Certains fournisseurs de services numériques – les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage – devront aussi prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales. Les exigences de sécurité et de notification sont, cependant, plus légères pour ces fournisseurs. Les micro- et petites entreprises numériques seront exemptées de ces exigences.

Mécanismes de coopération à l'échelle européenne

Les nouvelles règles prévoient un « groupe de coopération » stratégique pour échanger l'information et aider les États membres à renforcer leurs capacités en matière de cybersécurité. Chaque pays de l'Union devra adopter une stratégie nationale relative à sécurité des réseaux et des systèmes d'information.

Les États membres devront aussi mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) pour gérer incidents et risques, discuter des questions de sécurité transfrontalière et identifier des réponses coordonnées. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) jouera un rôle clé dans la mise en œuvre de la directive, en particulier en matière de coopération. La nécessité de respecter les règles de protection des données est réitérée tout au long de la directive.

Prochaines étapes

La directive sur la sécurité des réseaux et des systèmes d'information sera bientôt publiée au Journal officiel de l'Union européenne et entrera en vigueur le vingtième jour suivant sa publication. Les États membres auront alors 21 mois pour transposer la directive dans leur législation nationale et six mois supplémentaires pour identifier les opérateurs de services essentiels.

Directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Procédure: codécision, seconde lecture
Source : Parlement européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité: les députés soutiennent les règles pour aider les entreprises de services clés à… – Linkis.com

---

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
« N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle. »

Jean-Jacques Urvoas, ministre de la Justice, au Sénat

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « données contenues dans tout système informatique présent sur les lieux de la perquisition », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « données accessibles à partir du système initial ou disponibles pour le système initial », qui a disparu.

« Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les **données contenues dans tout système informatique ou équipement terminal présent sur les lieux** de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.
La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui **en indique les motifs** et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition. **À compter de la saisie, nul n'y a accès avant l'autorisation du juge.**
L'autorité administrative **demande au juge des référés du tribunal administratif d'autoriser en tant sa partie leur exploitation.** Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il **statue dans un délai de quarante-huit heures** à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative. **Sont exclus de l'autorisation les éléments découverts de tout lien avec la menace** que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics. **En cas de refus** du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa, **les données copiées sont détruites** et les supports saisis sont restitués à leur propriétaire.
Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont **restitués à leur propriétaire**, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent, **à l'issue d'un délai maximal de quinze jours** à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent. **À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les données copiées sont détruites à l'expiration d'un délai maximal de trois mois** à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.
En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. **Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables** en matière de procédure pénale.
Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. **Ses décisions sont susceptibles d'appel** devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article. »
Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.
Article original de Guillaume Champeau

Original de l'article mis en page : État d'urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

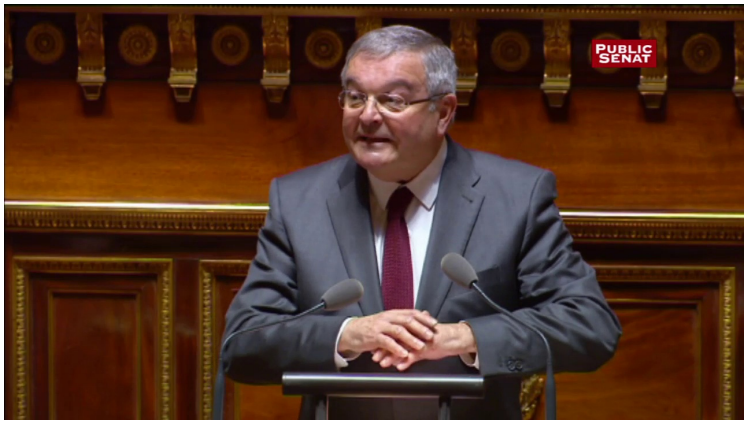
Quelles sont les limites d'accès aux données de connexion en situation d'État d'urgence ?

Quelles sont les limites d'accès aux données de connexion en situation d'État d'urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama

---

Sanction de la CNIL pour BrandAlley.fr

Sanction de la CNIL pour BrandAlley.fr

La CNIL vient d'infliger une sanction administrative de 30 000 euros à l'encontre de BrandAlley.fr. La société éponyme, derrière ce site de ventes en ligne, est épinglée pour plusieurs indélicatesses à l'égard de la loi de 1978.

Le 13 janvier 2015, une délégation de la CNIL effectuait un premier contrôle sur place pour relever déjà différents manquements de cette société française. Cela aurait pu en rester là si tout avait été rectifié à temps, mais en mars de la même année, une cliente a saisi la CNIL pour se plaindre de difficultés dans l'exercice de son droit d'accès aux données personnelles. Cette internaute adressait d'ailleurs au site de e-commerce une nouvelle lettre en mai 2015, sans plus d'effet.
Le 3 juillet 2015, BrandAlley était du coup mise en demeure par la CNIL de corriger plusieurs points de son système dans les trois mois. Bon prince, la Commission lui accordait un peu plus tard une rallonge de trois nouveaux mois. Les points litigieux visent à :
• Encadrer le traitement relatif à la prévention des fraudes,
• Mettre en place d'une durée de conservation des données clients,
• Recueillir le consentement préalable des clients pour la conservation des données bancaires,
• Prendre en compte de la demande de la plaignante,
• Obtenir l'accord des internautes s'agissant des cookies,
• Cesser de transmettre les données à caractère personnel vers des pays hors UE qui n'assurent pas un niveau suffisant de protection de la vie privée et des libertés et droits fondamentaux.

Dans un courrier de janvier 2016, BrandAllay affirmait à la CNIL qu'elle s'était désormais mise en conformité. Peu satisfaite des réponses « lacunaires », la Commission organisait un nouveau contrôle sur place en février 2016. Contrôle qui a montré la persistance de plusieurs problèmes déjà relevés. En outre, un mois plus tard, elle a effectué un contrôle à distance du site Internet, une possibilité accordée par la loi sur la consommation.
La procédure gagnait alors un tour de vis supplémentaire. La CNIL a désigné un rapporteur, en l'occurrence François Pellegrini, une étape préalable à toute sanction où la société peut encore donner ses explications. Dans ce document désormais public , le rapporteur a constaté plusieurs défauts.

Des réactions trop tardives

Premièrement, BrandAllay.fr n'avait pas déposé dans le délai imparti, de demande d'autorisation pour la mise en œuvre d'un traitement antifraude. Selon les éléments du dossier, c'est « la réception du rapport de sanction qui a conduit la société à effectuer une demande d'autorisation ». Mais beaucoup trop tardivement pour ne pas abuser de la patience de l'autorité administrative…
S'agissant de la durée de conservation des données personnelles, on se retrouve un peu dans même situation. À l'échéance du délai imparti, la société avait indiqué s'être conformé à la norme simplifie 48, celle relative à la gestion de clients et de prospects. Dans le même temps, elle ajoutait que les données clients seraient conservées 5 années durant, à compter de la fin de la relation commerciale. Or ce délai non prévu par la norme en question. Pire, lors du deuxième contrôle sur place, la CNIL a constaté qu' « aucune purge des données n'avait été réalisée ». Les explications fournies par le site de e-commerce – liées à la complexité de mise en œuvre – n'ont pas eu de poids, même si elle a depuis corrigé le tir pour revenir à un délai de conservation de 3 ans.

Cookies, chiffrement, Maroc et Tunisie

S'agissant des cookies, la société mise en demeure avait informé l'autorité de la mise en place un bandeau afin de recueillir le consentement des internautes, avant dépôt de cookies. Le contrôle en ligne effectué en mars 2016 a révélé la solidité de cette affirmation. D'un, le fameux bandeau « était rédigé de telle sorte qu'il n'informait pas les utilisateurs de leur possibilité de paramétrer le dépôt de cookies ». Soit un joli manquement à l'article 32-II de la loi de 1978.
De deux, des cookies à finalités publicitaires étaient déposés dès l'arrivée sur le site, sans l'ombre d'un consentement préalable. Pour ce dernier point, la CNIL n'a finalement pas retenu de grief, s'estimant « insuffisamment éclairée (…) sur la répartition exacte des responsabilités entre l'éditeur du site, les annonceurs et les régies publicitaires concernés ». Par constat d'huissier, BrandAlley a par ailleurs démontré s'être mise depuis d'aplomb.
Ce n'est pas tout. La CNIL a pareillement dénoncé l'absence de chiffrement du canal de communication et d'authentification lors de l'accès à BrandAlley.fr (usage du HTTP, plutôt que HTTPS). Le 29 mars 2016, la société a produit un nouveau constat d'huissier pour montrer à la CNIL que ce défaut se conjuguait désormais au passé. Un peu tard là encore pour la Commission qui a relevé un nouveau manquement.
Enfin, la société transférait vers le Maroc et la Tunisie les données personnelles de ses clients, via l'un de ses sous-traitants. Malgré des affirmations en sens contraire en janvier 2016, la CNIL a relevé en février la persistance de ces transferts. Or, en principe, de telles opérations ne sont possibles que si le pays de destination offre un niveau de protection comparable à celui en vigueur en Europe, ce qui n'était pas le cas ici (pas plus qu'aux Etats-Unis depuis l'invalidation du Safe Harbor par la justice européenne).
Après délibération, la CNIL a décidé de sanctionner la société de 30 000 euros d'amende, outre de rendre public la délibération. Une sanction loin d'être négligeable, le critère de la confiance sur Internet étant cruciale pour un site de e-commerce. La société peut maintenant attaquer, si elle le souhaite, la décision devant le Conseil d'État.

Article original de Marc Rees

Réagissez à cet article

Original de l’article mis en page : Données personnelles : BrandAlley.fr sanctionné par la CNIL

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

En cette période de pause estivale propice aux voyages, nombreux sont ceux qui ont réservé une chambre d'hôtel sur un site internet ou s'apprêtent à poster sur Facebook leurs photos souvenirs. Parmi ces personnes, combien s'interrogeront sur l'utilisation qui peut être faite des données quils auront ainsi (bien involontairement) transmises?

Cette question est au cœur de la problématique de la protection des données personnelles, qui intéresse l'Union européenne, notamment lorsque le transfert se fait d'un pays européen vers un pays tiers. Le principe veut que ce type de transfert de données à caractère personnel vers un pays tiers soit interdit, sauf si le pays en question assure un niveau de protection suffisant pour ces informations.

En juin 2013, les révélations d'Edward Snowden sur la récupération par l'agence de renseignements américaine, la NSA (National Security Agency), des données personnelles des citoyens européens, et donc leur surveillance par les autorités américaines, ont conduit l'UE à revoir les accords existants sur le sujet.

Alors que les négociations étaient en cours, une décision de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015, a précipité le processus. La Cour avait à se prononcer sur une question posée par la Haute Cour de justice irlandaise relative à la validité des principes dits Safe Harbor (sphère de sécurité). Ceux-ci étaient énoncés dans la décision de la Commission européenne du 26 juillet 2000 dans laquelle elle considérait que les Etats-Unis assuraient un niveau suffisant de protection des données personnelles pour permettre le transfert des données.

Mais la Cour de justice de l'Union européenne a invalidé cette décision. Marquée par les révélations de l'affaire Snowden, elle a constaté que le régime américain de protection des données personnelles « rend possible des ingérences (…) dans les droits fondamentaux des personnes » par les autorités publiques américaines.

La négociation d'un nouvel accord devenait urgente pour les quelques 4.000 entreprises soumises au Safe Harbor devenu caduc et laissant donc place à un vide juridique. Or, le sujet de l'utilisation des données personnelles est particulièrement brûlant quand on connait la valeur de celles-ci pour les entreprises: l'exploitation des données personnelles de ses utilisateurs aurait rapporté 12 milliards de dollars à Facebook en 2014, selon Les Echos.

Le nouveau dispositif, baptisé Privacy Shield (bouclier de protection de la vie privée), a été négocié entre la Commission européenne et les Etats-Unis, qui sont parvenus à un accord le 2 février 2016. Le 13 avril, les autorités européennes de protection des données (la CNIL pour la France) ont émis un avis sur cet accord, où elles expriment de sérieuses préoccupations. Puis le Parlement européen a fait de même dans une résolution votée le 26 mai: les députés européens réclamait de rouvrir les négociations pour apporter plus de garanties. Le 8 juillet, les Etats membres, réunis au sein d'un groupe de travail, ont quant à eux validé le texte, malgré l'abstention de quatre pays, l'Autriche, la Hongrie, la Slovénie et la Bulgarie.

Finalement, le 12 juillet 2016, la Commission européenne adopte sa décision relative au bouclier de protection des données UE-Etats-Unis. La commissaire européenne chargée de la Justice, des Consommateurs et de l'Egalité des genres, Věra Jourová, a déclaré que le Privacy Shield est « un nouveau système solide destiné à protéger les données à caractère personnel des Européens et à procurer une sécurité juridique aux entreprises. Il prévoit des normes renforcées en matière de protection des données, assorties de contrôles plus rigoureux visant à en assurer le respect, ainsi que des garanties en ce qui concerne l'accès des pouvoirs publics aux données et des possibilités simplifiées de recours pour les particuliers en cas de plainte. Le nouveau cadre rétablira la confiance des consommateurs dans le contexte du transfert transatlantique de données les concernant ».

Ainsi, le nouveau système se veut plus protecteur que la précédente « sphère de sécurité »: la collecte des données par les sociétés américaines ne peut notamment pas être utilisée pour des usages non prévus initialement. Egalement, un médiateur aux Etats-Unis sera chargé de recevoir les plaintes des Européens. Tous les ans, la Commission examinera le respect du dispositif par les Etats-Unis.

Toutefois, le bouclier peine à convaincre. Les services de renseignements américains peuvent continuer à intercepter les données personnelles des Européens. Les associations fustigent un accord jugé largement insuffisant, qualifié de bouclier troué par la Quadrature du net. Du côté des députés européens, si la droite (les groupes PPE et CRE) est satisfaite, ce n'est pas le cas des Socialistes, des Verts et des Libéraux. Eux estiment que le nouveau système ne respecte pas les exigences posées par la CJUE: « la CJUE a dit que le problème, c'était les lois américaines. Or rien, dans les textes américains, n'a changé », pointe Jan Philipp Albrecht (Verts).

Le nouvel accord est par conséquent susceptible d'être à nouveau invalidé par les juges européens. Pour finir, il a été élaboré dans le cadre de la directive européenne de 1995 sur la protection des données. Or, cette directive va être remplacée en mai 2018 par un règlement adopté en 2015. L'insécurité juridique, ennemi des entreprises, plane donc toujours. Quant aux citoyens, ils ne peuvent que déplorer que la protection de leur vie personnelle soit mise en balance avec des enjeux économiques et de sécurité.

Avec la contribution de la Maison de l'Europe de Paris

Réagissez à cet article

Original de l’article mis en page : Protection des données personnelles: lautre pomme de discorde entre lUnion européenne et les Etats-Unis | www.francesoir.fr

---

De nouvelles investigations sur l’IP Tracking en préparation

De nouvelles investigations sur l’IP Tracking en préparation

Les cybermarchands sont prévenus : la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) va mener « dans les prochains mois » de nouvelles investigations relatives à l'IP Tracking, cette technique de pistage dont aucun cas avéré n'avait été détecté lors d'une précédente enquête, remontant à 2013.

Certains sites de e-commerce modulent-ils leurs tarifs en fonction du nombre de visites de leurs utilisateurs ? C'est en tout cas ce que soutiennent de nombreuses personnes, au motif que le prix de certains articles augmenterait artificiellement en cas de consultations à répétition d'un même article. Le but : faire croire au consommateur que les biens restants (des billets d'avion ou des chambres d'hôtel par exemple) diminuent et qu'il faut donc passer commande sans tarder… Cette technique est généralement appelée « IP Tracking », dans la mesure où elle repose sur la reconnaissance de l'adresse IP de la connexion utilisée.

La pratique reste toutefois « *difficile à qualifier juridiquement et difficile également à démontrer* » selon Martine Pinville, la secrétaire d'État au Commerce. Interpellée par un sénateur qui lui avait transmis une question écrite en juillet 2015, l'intéressée rappelle que l'enquête menée à ce sujet en 2013 par la CNIL et la DGCCRF était ainsi arrivée à la conclusion qu' « *aucune des techniques observées ne prenait en compte l'adresse IP des internautes comme élément déterminant ou ne visait à moduler le prix des produits ou services proposés aux consommateurs* ».

Aucune plainte de consommateurs enregistrée par la DGCCRF

Pour l'heure, poursuit Martine Pinville, « *la DGCCRF n'a pas été saisie de plaintes de consommateurs concernant des pratiques « d'IP tracking »* ». Bercy n'aurait pas non plus « *eu connaissance de signalements de cette nature* » au sein du réseau de coopération administrative du « G29 » des CNIL européennes.

La secrétaire d'État cherche néanmoins à rassurer : elle annonce que « *le sujet de « l'IP tracking » fera l'objet dans les prochains mois de nouvelles investigations* » de la part de la DGCCRF. Si de telles pratiques venaient à être débusquées, les cybermarchands concernés pourraient être poursuivis pour pratiques commerciales déloyales ou trompeuses, explique Martine Pinville, car « *susceptible[s] d'altérer le comportement économique du consommateur* ». Les contrevenants s'exposeraient alors à des peines pouvant aller jusqu'à deux ans de prison et 300 000 euros d'amende.

Un front pourrait également s'ouvrir en matière de protection des données personnelles. « *L'adresse IP étant une donnée personnelle, il faudrait avant toute exploitation, demander l'accord et le consentement du consommateur ainsi que la déclaration de ces données à la CNIL, en respectant la procédure requise : durée de conservation des données, finalité, etc.* »

Article original de Xavier Berne

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : IP Tracking : de nouvelles investigations de la répression des fraudes

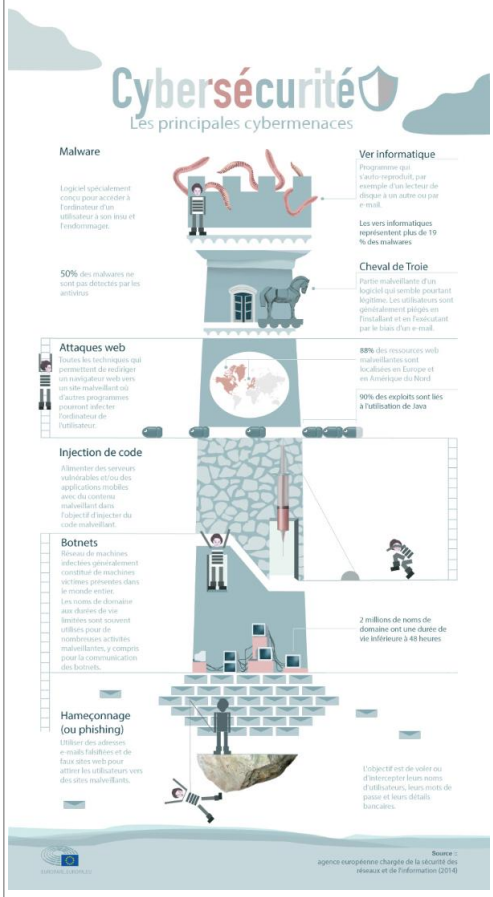
---

Directive sur la sécurité des réseaux et des systèmes

d’information

Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.



Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne

---

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

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

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

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

L’accord sur la transmission des données validé par la Commission Européenne

L’accord sur la transmission des données validé par la Commission Européenne – Filière 3e

---

Le 8 juillet, la Commission européenne a validé le projet des représentants des Etats-membres de l'UE et des Etats Unis sur le transfert des données en ligne. Une législation qui pourrait favoriser l'Open Data, les objets connectés ainsi que la mise en place de projets de transition énergétique.

A l'origine l'accord sur la transmission des données était appelé « Safe Harbour ». La Cour de Justice de l'Union européenne (CJUE) avait invalidé le texte en octobre 2015 en raison de sa faible sécurité pour les données personnelles. Après des mois de débats, l'accord sur la « protection de la vie privée » (Privacy Shield) a été approuvé par les Etats membres et est entré en vigueur le 11 juillet 2016. Il a pour but de faciliter le transfert des données entre les Etats-Unis et l'Union européenne dans le cadre de la signature du Traité Transatlantique (TAFTA ou TIPP). Ce texte a pour but de faciliter les échanges économiques entre l'UE et les Etats-Unis, en harmonisant les normes européennes à celles américaines. Ces échanges serviraient à encadrer le progrès dans la croissance économique, en favorisant les flux correspondant au secteur du numérique. Dans un communiqué de presse, Andrus Ansip, membre désigné de la Commission Juncker comme vice-président chargé du marché numérique, et la commissaire à la Justice, Vera Jourva, ont déclaré communément : « le texte est fondamentalement différent de l'ancien Safe Harbour: il impose des obligations claires et fortes aux entreprises traitant les données et s'assure que ces règles sont suivies et mises en pratique ».

L'Open Data utile à la transition énergétique ?

Largement décriée, la récupération des données servira pourtant à construire le monde de demain en s'inscrivant dans une logique de transition énergétique. Ainsi les villes, les maisons et les énergies fonctionneront dans un même système connecté et durable. Nombreuses sont les start-up a créer des applications facilitant la mobilité, la sécurité et l'habitat dans le cadre de projets « verts ». Les données deviennent un facteur important du marché économique et énergétique. Pour Christian Buchel, Directeur général adjoint, Chef digital et international pour le groupe ENEDIS : « l'Open Data est utilisé dans le monde entier. Humaniser la DATA c'est mieux comprendre la consommation générale d'énergie ». Des informations qui pourraient être utilisées à grande échelle afin d'accroître la capacité de gestion des énergies. L'anonymat des données serait préservé puisque seul le consommateur aurait accès à ses informations. Pour Sampo Hietanen, de MAAS Finlande, une entreprise spécialisée dans l'Open DATA, il faut « générer de l'information pour construire la ville de demain afin que les services proposés communiquent ensemble ».
Les Etats Unis ont déjà commencé à déployer ce système numérique avec la mise en place de compteurs intelligents, récupérant les données des citoyens pour adapter la consommation énergétique à la demande. La France et ERDF commencent à commercialiser Linky, le compteur intelligent français. En ce sens, la signature du Traité Transatlantique devrait favorisait les partenariats énergétiques et numériques entre l'Union Européenne et les Etats-Unis.
Article original de Mailys Kerhoas

Réagissez à cet article

Original de l'article mis en page : L'accord sur la transmission des données validé par la Commission Européenne – Filière 3e

---

L'Internet russe prêt à

ériger des frontières

L’Internet russe prêt à ériger des frontières

La Russie prévoit de contrôler davantage la partie russe du réseau Internet et son trafic, y compris l'activité des serveurs DNS et l'attribution des adresses IP.

L'an dernier, la Russie a annoncé l'entrée en vigueur d'une loi obligeant toute organisation détenant des données de citoyens russes à les stocker sur des serveurs se trouvant physiquement sur le territoire russe. Cette année, un autre projet de loi concocté par le ministère russe des communications, prévoit la création d'un système de surveillance du trafic Internet, y compris l'activité des serveurs DNS (système de noms de domaine) et l'attribution des adresses IP.
Le texte, dont le journal *Vedomosti* s'est fait l'écho, vise à réguler *« la partie russe du réseau Internet »*. Et ce officiellement pour renforcer la protection de l'Internet russe face aux cyberattaques. Le projet implique aussi la surveillance du trafic Internet transfrontalier, en s'appuyant notamment sur le système SORM (système pour activité d'enquête opératoire). Reste à savoir si la Russie a les moyens de faire appliquer de telles restrictions, dont elle devra mesurer l'impact économique.

Réseau de réseaux

Dave Allen, vice-président et avocat général de Dyn, un spécialiste de la performance réseau basé dans le New Hampshire, aux États-Unis, a publié une tribune sur le sujet dans *Venturebeat*. Allen observe qu'une grande partie du trafic Internet russe dépend actuellement beaucoup de pays avec lesquels la Russie entretient des relations compliquées, voire conflictuelles.
Les données partagées de Moscou à Saint-Pétersbourg par un abonné de l'opérateur mobile russe MegaFon, par exemple, transitent 9 fois sur 10 par Kiev, en Ukraine, selon lui. Et plus de 40 % des données qui passent par le réseau de MTS, le premier opérateur mobile russe, pour aller aussi à Saint-Pétersbourg, transiteraient par Amsterdam aux Pays-Bas et par Francfort en Allemagne.
La tendance se vérifie auprès d'entreprises publiques : ainsi, plus de 85 % des données transmises de Moscou vers Saint-Pétersbourg par TransTelekom, filiale de la Compagnie des chemins de fer russes, passeraient par Francfort. Et la plupart des données qui quittent la Russie, selon Dave Allen, passent par le backbone RETN, qui a des points de présence en Europe centrale et orientale.

Localisation de données

Les mesures de renforcement de la protection des données russes s'appliquent à toutes les entreprises ayant une activité dans le pays. L'an dernier, le régulateur russe Roskomnadzor a mené un audit auprès de 317 sociétés et administrations. Il a estimé que 2 étaient dans l'illégalité. L'audit pourrait être étendu cette année à d'autres grands groupes, dont Microsoft, HPE et Citibank.
Pour que les données puissent être transférées temporairement à l'étranger, une protection *« adéquate »* de ces données doit exister. L'Ukraine, l'Allemagne et les Pays-Bas ont signé une convention sur le traitement automatisé de données personnelles qui semble satisfaire cette condition. En revanche, le doute persiste sur le chiffrement. Le gouvernement russe, comme d'autres, envisage de l'affaiblir pour donner plus de marge de manoeuvre à ses services de renseignement.
D'autres pays ont fait des propositions en faveur de la localisation de données. En France, un amendement qui prévoyait l'interdiction de traitement de données personnelles stockées hors d'un État membre de l'Union européenne, a finalement été écarté du projet de loi République numérique.
Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : L'Internet russe prêt à

ériger des frontières