Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

En proposant de nouvelles règles télécom cette semaine, la Commission européenne introduirait des obligations de sécurité aux services de messagerie. Des obligations déjà en vigueur pour les opérateurs, qui réclament une parité réglementaire avec les acteurs en ligne.

Équilibrer les obligations entre opérateurs et messageries en ligne ressemble souvent à un travail de funambule, dans lequel se lancerait la Commission européenne. Dans quelques jours, l'institution doit dévoiler une révision des règles télécoms en Europe. Selon un brouillon obtenu par Reuters, elle y introduirait des obligations de sécurité pour les services de messagerie en ligne, déjà appliquées par les opérateurs.

Des obligations de signalement des brèches

À la mi-août, plusieurs médias affirmaient que la Commission européenne comptait proposer cette parité entre acteurs. Le brouillon obtenu par Reuters viendrait donc confirmer cette piste. Dans celui-ci, les services « over the top » devront ainsi signaler les brèches « *qui ont un impact important sur leur activité* » aux autorités et disposer d'un plan de continuité de l'activité. Les services qui proposent des numéros de téléphone ou d'en appeler, comme Skype, devront aussi permettre les appels d'urgence.

Pourtant, ces règles pourront être plus légères pour ces services que pour les opérateurs classiques, dans la mesure où les services ne maîtrisent pas complètement la transmission des contenus via les tuyaux. Dans l'absolu, ces règles doivent réduire l'écart d'obligations entre les acteurs télécoms et ceux d'Internet, avec en toile de fond le combat entre des acteurs européens et des sociétés principalement américaines.

Rappelons que le règlement sur les données personnelles, voté en avril par le Parlement européen, doit lui aussi obliger les services à divulguer aux autorités les fuites de données, dans un délai court. En France, cette obligation ne concerne que les opérateurs.

Le moment est d'ailleurs pour celle-ci, le secteur télécom étant notamment le théâtre de lobbyings intenses. Elle a d'ailleursretiré une proposition de « fair use » pour la fin des frais d'itinérance il y a quelques jours, suite à des levées de bouclier du côté des associations de consommateurs, des opérateurs et des eurodéputés. Comme le rappelle Reuters, ce texte passera entre les mains du Parlement et du Conseil de l'Europe, avec des changements possibles à la clé…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’UE préparerait l’extension de règles de sécurité des opérateurs aux acteurs du Net

---

CNIL : nouvelle norme simplifiée pour la scolarité des mineurs

	**CNIL : nouvelle norme simplifiée pour la scolarité des mineurs**

Dans le cadre de son programme de simplification des formalités préalables pour les collectivités territoriales, la Cnil a adopté une norme simplifiée unique qui met à jour et abroge le cadre existant.

Le 10 décembre 2015, la Commission a adopté une norme simplifiée n°NS-058 qui fusionne et abroge les normes simplifiées n°NS-027 et n°NS-033. En effet, ces normes étaient désuètes et ne répondaient pas aux nouvelles préoccupations des acteurs concernés. Elle a été présentée sur le site de la Cnil le 12 août dernier.
Cette nouvelle norme permet de simplifier, pour ces traitements courants, les démarches des collectivités territoriales et des organismes en charge d'un service scolaire, périscolaire et de petite enfance. Elle offre un cadre unifié et adapté aux contraintes liée à la gestion de ces services.
Après avoir vérifié que leur traitement s'inscrit précisément dans le champ d'application de cette norme, les responsables de traitements de données concernés devront effectuer un engagement de conformité à la norme NS-058 auprès de la CNIL.

Les personnes concernées

Cette norme s'adresse aux collectivités territoriales, aux personnes morales de droit public et aux personnes morales de droit privé gérant un service public…[lire la suite]

En savoir plus

Le communiqué de la Cnil du 12 août dernier avec une présentation synthétique de la norme :
https://www.cnil.fr/fr/une-nouvelle-norme-simplifiee-ns-058-pour-la-gestion-des-affaires-scolaires-periscolaires
Le résumé succinct de la norme :
https://www.cnil.fr/fr/declaration/ns-058-affaires-scolaires-periscolaires-extrascolaires-et-petite-enfance
La norme NS-058 elle-même sur *Légifrance* :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032788919

Réagissez à cet article

Original de l'article mis en page : Données personnelles : nouvelle norme simplifiée pour la scolarité des mineurs

Protection des données personnelles, plus que quelques mois pour se mettre en règle…

Protection des données personnelles, plus que quelques mois pour se mettre en règle…

Il y a urgence à se former aux nouvelles obligations en matière de protection des données… Après 4 années de négociations très médiatisées, le nouveau règlement européen de protection des données a été adopté en mai 2016. Il sera applicable en France le 25 mai 2018. Mais une bonne moitié des organisations françaises ne sont toujours pas informées du contenu de la réforme concernant la protection des données.

Pourtant, il y a de vraies conséquences en termes de responsabilités et de sanctions ! En cas de violation des dispositions du règlement, les pénalités peuvent atteindre un montant maximal de 4% du CA mondial d'un groupe ou de 20 Millions d'euros.

De plus, tout organisme public ou privé victime d'un piratage, d'une faille de sécurité ou de tout acte risquant de compromettre ou ayant compromis la sécurité (confidentialité, intégrité) de données personnelles aura 72 heures pour signaler l'incident à la CNIL.
L'organisme devra, dans la plupart des cas informer les victimes (comme Orange a été obligé de le faire à deux reprise en 2014).
Pas bon pour l'image ça !
Imaginez, des années pour construire votre réputation et en quelques heures :
1. Vous devez signaler à la CNIL que vous vous êtes fais pirater et que des données personnelles ont été compromises ;
2. Vous allez très probablement avoir droit à un contrôle de la CNIL qui va venir rechercher la cause de cette faille et par la même occasion faire le point sur votre mise en conformité ;
3. Pour couronner le tout (le 3ème effet Kiss Cool), vous risquez d'informer vos clients, salariés, fournisseurs que leurs données personnes ont été piratées sur votre système informatique. Imaginez leur réaction !!! Toujours pas bon pour l'image ça !

La première étape pour se mettre en conformité est de s'informer et de sensibiliser le personnel qui a un rôle important à jouer dans cette mise sur rail.
Ensuite, il sera nécessaire de former une personne en particulier dans votre établissement. Actuellement il s'appellera CIL (Correspondant Informatique et Libertés), demain DPO (Délégué à la Protection des Données), cette personne va jouer un rôle clé dans votre mise en conformoté.
Il devra :
1. Contrôler le respect du règlement ;
2. Informer et conseiller le responsable du traitement (ou le sous-traitant en charge de cette mission) et les employés qui procèdent au traitement des données sur les obligations qui leur incombent.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

Directive NIS adoptée: quelles conséquences pour les entreprises?

Directive NIS depuis juillet. Des changements pour les entreprises?

En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne
Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

---

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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.

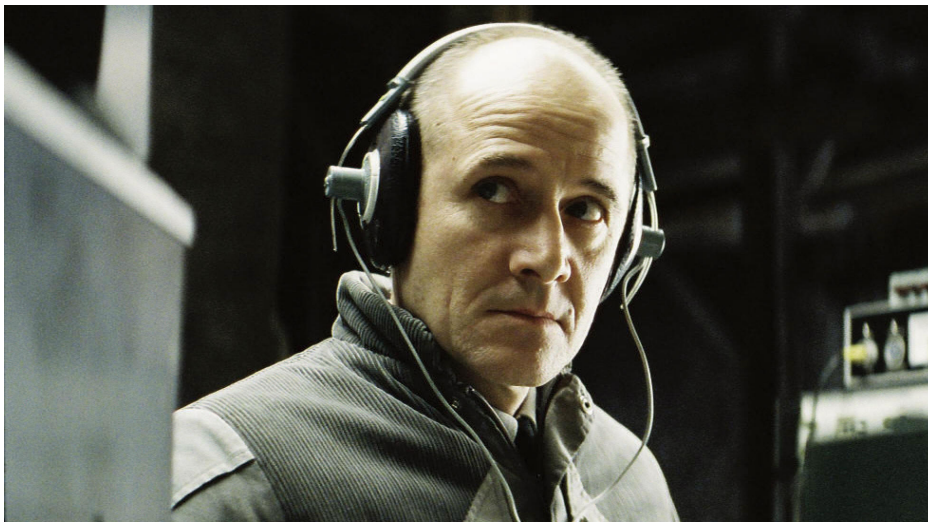
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Directive NIS adoptée: quelles conséquences pour les entreprises?

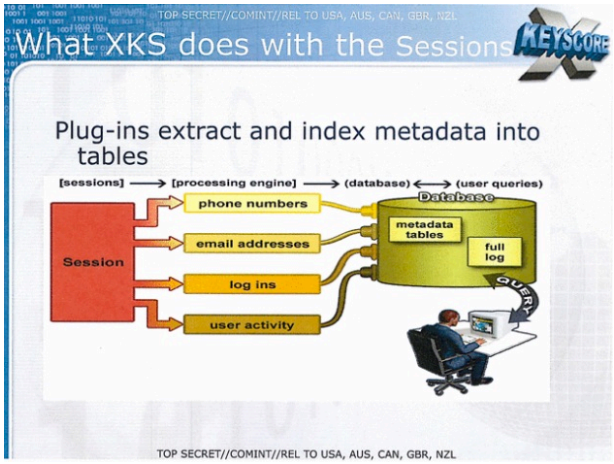
Collectes massives et illégales par le Renseignement allemand

	Collectes massives et illégales par le Renseignement allemand

---

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.



Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Retrouver l’auteur d’un E-mail à partir de l’adresse IP : Le demandeur condamné

Le TGI de Meaux a débouté l'entreprise qui voulait obtenir de Numericable les noms, prénoms, adresses et coordonnées complètes de l'auteur d'un email frauduleux à partir de son adresse IP.

Dans une ordonnance de référé du 10 août 2016 repérée par Legalis, le tribunal de grande instance de Meaux (Seine-et-Marne) a débouté l'entreprise qui voulait obtenir de Numericable les données d'identification correspondant à l'adresse IP de l'auteur présumé d'un email frauduleux.
Comment en est-on arrivé là ? En début d'année, la société France Sécurité a préparé une proposition commerciale à l'attention d'Airbus Helicopters dans le cadre d'un appel d'offres. Dans la foulée, le distributeur d'équipements de protection individuelle a reçu un courriel d'un individu se faisant passer pour un employé d'Airbus et lui demandant de transmettre par courriel le fichier contenant la proposition… Suspectant la fraude, France Sécurité a contacté Airbus. Le nom associé au courriel était bien celui d'un de ses employés, mais il n'était pas l'auteur des courriels en question.

Usurpation d'identité
Dans un premier temps, une plainte a été déposée contre X pour usurpation d'identité. Parallèlement, le département informatique de France Sécurité a identifié l'adresse IP de l'expéditeur du courriel (transmis via Gmail) ainsi que le FAI hôte, à savoir : Numericable. Un procès-verbal de constat d'huissier a été établi. Ensuite, le 28 juin 2016, France Sécurité a déposé plainte auprès du procureur de la République près le tribunal de grande instance de Nantes. Et le 8 juillet 2016, l'entreprise a fait assigner devant le juge des référés du TGI de Meaux le câblo-opérateur. Le but : obtenir du tribunal qu'il ordonne au FAI de communiquer dans un délai de 48 heures les données d'identification correspondant à l'adresse IP en cause. Car, selon le demandeur, le câblo-opérateur est tenu de conserver les données permettant l'identification de son client et de déférer aux demandes de l'autorité judiciaire. Et ce en application de la loi pour la confiance dans l'économie numérique (LCEN) du 21 juin 2004. France Sécurité souhaitait également qu'une astreinte soit versée par Numericable en cas de dépassement de ce délai, en plus des frais irrépétibles… Sans succès.

L'adresse IP, une donnée personnelle
Le juge est parti du principe que l'adresse IP est une donnée à caractère personnel. Par ailleurs, il a considéré que la collecte de cette donnée constitue un traitement au sens de la loi informatique et libertés. Une telle collecte aurait donc dû faire l'objet d'une autorisation de la Commission nationale informatique et libertés (Cnil) accordée à France Sécurité. Cela n'a pas été le cas. Par ailleurs, le juge considère que le cadre juridique applicable dans ce dossier ne peut pas être celui de la LCEN de 2004. Selon lui, Numericable n'est pas visé en tant que « personne dont l'activité est d'offrir un accès à des services de communication au public » en relation avec « la création d'un contenu » en ligne.
Résultat : le TGI de Meaux a débouté France Sécurité de toutes ses demandes. L'entreprise a été condamnée aux entiers dépens et au versement de 2 000 euros au titre des frais irrépétibles…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : IP : Numericable n’a pas à communiquer les données d’identification

---

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

---

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031

Révélations sur de petits

piratages informatiques entre alliés…

Révélations sur de petits piratages informatiques entre alliés…

C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.

Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »

Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »

Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Comment se passera le passage du CIL au DPO lors de la mise en application du RGPD ?

	Comment se passera le passage du CIL au DPO lors de la mise en application du RGPD ?

Plus de vingt ans après la Directive sur la Protection des Données, l'Union Européenne s'est dotée ce printemps d'un nouveau règlement. Les deux décennies passées ont vu des changements phénoménaux dans nos usages du numérique. Le texte, issu d'un délicat compromis entre les institutions européennes et les acteurs du numérique, prend acte de ces changements (en entérinant par exemple le célèbre « droit à l'oubli ») et trace le futur de la protection des données en Europe, notamment en mettant au centre de son texte un acteur nouveau, ou en tout cas ré-inventé, le Data Protection Officer (DPO). Mais au « jour J » de l'entrée en application du texte, qui seront les DPO ? Quelles seront leurs missions, et comment s'y préparer dès maintenant ?

Le DPO, un « CIL 2.0 » ?

Le texte en français (pas encore officiel) du futur règlement européen ne traduit pas, à raison, « Data Protection Officer » par « Correspondant Informatique & Libertés », mais par « Délégué à la protection des données ». En effet, les futurs DPO auront des responsabilités plus diverses que les CIL, mais aussi plus lourdes. Les enjeux sont importants, puisque la CNIL, comme tous ses équivalents européens, pourra, grâce au nouveau règlement, imposer des sanctions financières équivalentes à ce que l'on peut observer en droit de la concurrence (jusqu'à 4 % du chiffre d'affaires annuel mondial). En termes de position, le DPO gagne également en reconnaissance, puisque le règlement stipule que « le délégué à la protection des données fait directement rapport au niveau le plus élevé du responsable de traitement ». Son identité devra également être rendue publique, à l'instar des responsables de l'accès aux documents administratifs désignés au titre de la loi CADA.

Cette montée en responsabilité, interne aussi bien qu'auprès du public, s'accompagnera vraisemblablement d'une hausse des salaires, pour rejoindre ceux que l'on observe en Amérique du Nord, par exemple, où une société dont la réputation fut salie par une affaire de data breach n'a pas hésité à rémunérer ensuite son nouveau CPO à hauteur de 700.000 $ par an pour regagner la confiance de ses clients.

La principale évolution entre CIL et DPO, cependant, demeure dans l'étendue de leur champ d'action. Aux tâches déjà accomplies par le CIL s'ajoutent, pour le DPO, celles de notification et d'enregistrement des violations de données personnelles, ainsi que des analyses d'impact de ces violations, entre autres.

Du CIL au DPO : une transition légitime

Les similarités entre CIL et DPO sont nombreuses, et les compétences, ainsi que l'expérience, accumulée par les CIL ces dix dernières années seront un formidable atout pour aborder les changements qui s'annoncent. Ainsi, pour capitaliser sur les travaux réalisés par les CIL déjà désignés et pour assurer la diffusion la plus large possible de l'esprit de la loi, l'AFCDP, association qui regroupe les professionnels de la conformité Informatique et Libertés et de la protection des données personnelles, demande que soit ménagée une « clause du grand-père » qui permettrait à ces CIL qui le souhaitent et qui répondent aux nouvelles exigences d'être maintenus dans leur fonction en tant que DPO. Par ailleurs, la CNIL soutient ce passage « naturel » du CIL au DPO, comme l'a confirmé Edouard Geffray, Secrétaire général de la CNIL devant les 500 CIL réunis fin janvier à l'occasion de la journée mondiale de la protection des données personnelles : *« Nous avons tout intérêt à ce que la plupart d'entre vous soient confirmés en tant que DPO ».*

Cela ne signifie en aucun cas que le milieu professionnel des CIL devrait refuser d'accueillir de nouveaux arrivants. Il en faudra, en effet, par conséquence logique de la multiplication attendue des postes, le DPO étant obligatoire dans de très nombreuses structures. Il faudra donc s'assurer qu'ils bénéficient de la culture de métier forte que les CIL se sont construites ces dernières années. En revanche, ce qu'il convient plutôt d'essayer de minimiser, c'est la possible délocalisation d'une partie des DPO hors de France. En effet, même si le règlement indique que « *Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement* », il est probable que certains grands groupes décident de localiser leur DPO en Grande-Bretagne, en Irlande, aux Pays-Bas ou en Belgique. Le revers de cette harmonisation européenne serait alors un éloignement croissant entre les citoyens et les responsables du traitement de leurs données à caractère personnel.

Deux précieuses années de préparation

Les nouvelles règles, appelées à remplacer celles de notre actuelle loi Informatique et Libertés, seront applicables le 25 mai 2018. Les organismes ayant déjà désignés un CIL ont une longueur d'avance pour préparer la mise en application du règlement. Les deux années qui viennent seront l'occasion de mettre en place de nouveaux chantiers et de nouvelles pratiques qui, de par leurs nouveautés, vont demander du temps et de la préparation. Ainsi des notifications de violation du traitement des données à caractère personnel, qui devra se faire sans délai auprès de la CNIL, et, dans certaines conditions, auprès des personnes concernées. Cet exercice, qui mêle des compétences en communication, en sécurité et en droit, demande une préparation préalable importante, afin de respecter les délais et d'établir rapidement le dialogue entre les différents acteurs, externes aussi bien qu'internes. À ce titre, deux ans ne seront pas de trop pour préparer, former et communiquer avec les collaborateurs réguliers du CIL. Ce dernier peut aussi avoir intérêt à compléter si besoin sa formation, afin de se préparer au mieux à la transition et d'apparaître auprès de ses supérieurs comme solution naturelle pour remplir la fonction de DPO.

Cette préparation, si elle est conséquente, ne sera pas nécessairement solitaire. Outre les documents officiels appelés à approfondir et clarifier certains détails du texte, les CIL pourront s'appuyer sur leur travail mutuel, notamment l'AFCDP, qui dispose d'ores et déjà d'un groupe de réflexion, aussi bien numérique que physique, sur les nouveaux défis apportés par le règlement. Ce travail bénéficiera en outre du réseau CEDPO (*The Confederation of European Data Protection Organisations*, co-fondée par l'AFCDP) qui permet aux CIL français de profiter des expériences et des bonnes pratiques de leurs confrères allemands, espagnols, néerlandais, polonais, irlandais et autrichiens. Enfin, compte tenu du changement d'échelle et de logique qui s'annonce en matière de protection des données à caractère personnel, il est crucial que les organismes qui n'ont pas déjà désigné un CIL le fassent, pour être prêt en 2018 à faire face aux nouvelles exigences.

Article original de Paul-Olivier Gibert

Président de l'AFCDP

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 : Règlement européen Données personnelles : du CIL au Data Protection Officer, une transition… — Linkis.com

---

Privacy Shield adopté,

nouveau fondement pour les transferts de données outre-atlantique

Privacy Shield adopté, nouveau fondement pour les transferts de données outre-atlantique

La Commission européenne a adopté mardi 12 juillet dernier le Privacy Shield. Ce nouvel accord remplace le Safe Harbor, et aura pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis adhérant à ce dispositif.

L'adoption de ce nouveau « bouclier de protection des données personnelles » est l'aboutissement d'un long processus, commencé dès 2014, avec la révélation par l'ancien agent de la CIA Edward Snowden de la surveillance de masse effectuée par les services de renseignements américains puis par le refus, sur ce motif, d'un citoyen autrichien de transférer ses données vers les Etats-Unis. La Cour de Justice de l'Union Européenne a ainsi dans une décision du 6 octobre 2015 déclaré invalide la décision de la Commission du 26 juillet 2000 constatant que les Etats-Unis assurent un niveau de protection adéquat aux données caractère personnel transférées. En effet la Cour a considéré que les Etats-Unis n'apportaient pas les garanties suffisantes pour protéger les données des citoyens Européens au motif que les pouvoirs des services de renseignements américains s'étendaient à toutes données exportées depuis l'Europe dès lors que l'intérêt de sécurité publique était en cause. La CJUE a considéré que ces intrusions étaient disproportionnées et heurtaient les principes de la Charte des droits fondamentaux de l'Union Européenne.
A la suite de cette décision, l'ensemble des transferts de données personnelles vers des entités situés aux Etats-Unis sur le fondement du Safe Harbor ont dû être suspendus et des solutions alternatives mises en place. Le Groupe de travail de l'article 29, qui est constitué des différents autorités de protection des données à caractère personnel au sein de l'UE (le G29), a assuré les organisations souhaitant poursuivre le transfert de données de l'UE vers les Etats-Unis qu'elles pouvaient se fonder sur les mécanismes alternatifs prévus par la directive de 1995 relative à la protection des données, telles que les clauses contractuelles types et les règles d'entreprise contraignantes (BCR).
En parallèle la Commission européenne et le gouvernement américain engageaient des discussions afin de trouver un nouvel accord sur le transfert des données personnelles des citoyens européens vers les Etats-Unis.
Le 2 février 2016, la Commission européenne et le gouvernement des Etats-Unis sont parvenus à un premier accord politique. La Commission a présenté le projet d'accord le 29 février 2016. Le groupe de travail « Article 29" a ensuite rendu un premier avis le 13 avril 2016 assez critique en particulier sur l'insuffisance des gardes fous accordés aux citoyens européens pour contrôler l'usage de leurs données.
Une résolution a été adoptée le 26 mai par le Parlement européen, et la Commission a clôturé la procédure d'adoption du nouvel accord le 12 juillet 2016 en adoptant une décision d'adéquation visant à reconnaitre au mécanisme « EU-U.S. Privacy Shield » un niveau de protection « essentiellement équivalent » aux exigences européennes. .

Le nouveau dispositif : Comment ça marche ?

Le Privacy Shield vise à permettre aux entreprises de transférer plus facilement vers les Etats Unis des données personnelles collectées dans l'Union européenne, tout en protégeant les droits des personnes concernées.

Le Privacy Shield est fondé sur les principes suivants:
• Des obligations strictes pour les entreprises qui traitent des données : dans le cadre du nouveau dispositif, le ministère américain du commerce procédera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes, afin de veiller à ce qu'elles observent les règles auxquelles elles ont souscrit. Les entreprises dont la pratique ne sera pas conforme aux nouvelles règles s'exposeront à des sanctions et à une radiation de la liste des entreprises adhérant au dispositif.
• Un accès des pouvoirs publics américains soumis à des conditions claires et à des obligations de transparence : les Etats-Unis ont donné à l'Union européenne l'assurance que l'accès des pouvoirs publics aux données à des fins d'ordre public et de sécurité nationale serait soumis à des limitations, à des conditions et à des mécanismes de surveillance bien définis. De même, tous les citoyens de l'Union bénéficieront pour la première fois de mécanismes de recours dans ce domaine. Les Etats-Unis ont exclu toute surveillance de masse systématique des données à caractère personnel transférées vers leur territoire dans le cadre du bouclier de protection des données UE-Etats-Unis. Le secrétaire d'État américain a instauré une possibilité de recours pour les Européens dans le domaine du renseignement national en créant un mécanisme de médiation au sein du département d'État ;
• Une protection effective des droits individuels : tout citoyen estimant que les données le concernant ont fait l'objet d'une utilisation abusive dans le cadre du Privacy Shield bénéficiera de plusieurs mécanismes accessibles et abordables de règlement des litiges. Lorsqu'un litige n'aura pas été réglé par l'un de ces moyens, un mécanisme d'arbitrage sera disponible, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouvert aux citoyens de l'UE passera par un médiateur indépendant des services de renseignement des États-Unis ;
• Un mécanisme de réexamen annuel conjoint : ce mécanisme permettra de contrôler le fonctionnement du Privacy Shield, et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale. Le réexamen sera mené par la Commission européenne et le ministère américain du commerce, lesquels y associeront des experts nationaux du renseignement travaillant au sein des autorités américaines et européennes de protection des données. La Commission s'appuiera sur toutes les autres sources d'information disponibles et adressera un rapport public au Parlement européen et au Conseil.

Le Privacy Shield reste donc un mécanisme souple, à l'instar du Safe Harbor sous-tendu par une nécessité d'auto-certification des entreprises américaines. Pour bénéficier de l'accord et faciliter les transferts de données personnelles entre l'Europe et les Etats Unis, les entreprises américaines adhérant au dispositif devront s'engager à respecter les obligations de protection des données du Privacy Shield.
La décision « Privacy Shield » entrera en vigueur à compter de sa notification à chacun des Etats membres de l'Union européenne et sera contraignante pour ceux-ci. L'applicabilité de ce cadre juridique aux entreprises concernées sera ensuite subordonnée à l'enregistrement de celles-ci auprès des autorités américaines en charge de la mise en œuvre du dispositif. Les entreprises américaines pourront obtenir la certification Privacy Shield à partir du 1er août 2016.
Si un des objectifs poursuivi par le Privacy Shield est d'exclure tout traitement massif des données européennes transatlantique la collecte massive de données pourra cependant être effectuée si elle est limitée à des objectifs de sécurité nationale prédéfinis : espionnage, terrorisme, armes de destruction massive, menaces sur la cyber-sécurité, sur les armées, ou menaces criminelles transnationales.

Un accord déjà critiqué

En dépit de son objectif d'amélioration de la protection des données personnelles, le nouveau cadre fait pourtant l'objet de nombreuses critiques.
Le G29 dans son avis d'avril 2016 avait notamment fait part de ses préoccupations sur un certain nombre de points manquants, incomplets ou peu clairs. Le G29 avait en particulier regretté l'absence de plusieurs principes tels que la limitation de la durée de conservation et l'interdiction des décisions automatisées. En ce qui concerne l'accès par les autorités publiques aux données, le G29 avait déploré que les autorités américaines n'aient pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens. Enfin, le G29 avait émis des doutes sur l'indépendance du médiateur (Ombudsperson) et sur le fait qu'il dispose de pouvoirs suffisants pour exercer son rôle efficacement et permettre d'obtenir un recours satisfaisant en cas de désaccord avec l'administration.
Il n'est pas certain que la nouvelle rédaction satisfasse pleinement le G29.
De même le 30 mai 2016, le contrôleur européen de la protection des données (EDPS en anglais), Giovanni Buttarelli, dans un Avis sur le Privacy Shield, demandait des améliorations « significatives » avant son adoption par la Commission européenne (CE). Selon l'Avis de l'EDPS: « La proposition de Privacy Shield est un pas dans la bonne direction, mais dans sa rédaction actuelle elle ne prend pas suffisamment en compte, de notre point de vue, toutes les garanties appropriées pour protéger les droits européens des individus à la vie privée et à la protection des données notamment en ce qui concerne le recours juridictionnel. Des améliorations significatives sont nécessaires dans l'hypothèse où la Commission européenne souhaiterait adopter une décision d'adéquation ».
Le G29 mène actuellement une analyse de la décision de la Commission et se réunira le 25 juillet 2016 afin de finaliser sa position.
Article original de DLA PIPER

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.L.I. (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 : Adoption du Privacy Shield par la Commission européenne : un nouveau fondement pour les transferts de données outre-atlantique, Partenaire – Les Echos Business