L’ANSSI alerte sur les risques liés à Pokémon Go

L’ANSSI alerte sur les risques liés à Pokémon Go

Face au phénomène Pokémon Go, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) a publié un bulletin de sécurité sur l'installation et l'usage de cette application.

Devant l'ampleur du phénomène (près de 100 millions de téléchargements), l'application Pokémon Go pose quelques problèmes de sécurité. L'ANSSI (en quelque sorte le Gardien de la sécurité des Systèmes d'Information des Organisme d'Importance Vitale, des Organes et Entreprise de l'état Français selon Denis JACOPINI expert Informatique assermenté spécialisé en cybercriminalité) ne pouvait pas rester sourde à cette question et vient de publier via le CERT-FR un bulletin de sécurité dédié aux « *cyber-risques liés à l'installation et l'usage de l'application Pokémon Go* ».

Applications malveillantes et collectes de données

Dans ce bulletin, il est rappelé qu'avec le succès, de nombreuses fausses applications se sont créées. Le CERT-FR en a recensé 215 au 15 juillet 2016. Elles sont surtout présentes dans les pays où le jeu n'est pas présent. Il recommande donc de ne pas télécharger cette application sur des sites tiers, et de n'installer que les versions originales disponibles sur Google Play ou l'Apple Store. Nous nous étions fait l'écho de la disponibilité d'APK Pokémon Go pour Android qui contenait des malwares. Le bulletin constate aussi que Niantic a résolu le problème de permission qui exigeait un accès complet au profil Google de l'utilisateur.

Sur les données personnelles, l'ANSSI observe comme beaucoup d'autres organisations que Pokémon Go collecte en permanence de nombreuses données personnelles. Informations d'identité liées à un compte Google, position du joueur par GPS, etc. L'UFC-Que Choisir avait récemment alerté sur cette question de la collecte des données. La semaine dernière la CNIL a publié un document concernant « jeux sur votre smartphone, quand c'est gratuit… » où elle constatait que ce type d'application était très gourmande en données. L'ANSSI préconise la désactivation du mode « réalité augmentée » lors de la phase de capture d'un Pokémon.

BYOD et Pokémon Go, le pouvoir de dire non

L'ANSSI répond sur le lien qu'il peut y avoir entre le BYOD (Bring Your Own Device), c'est-à-dire l'utilisation de son terminal personnel dans un cadre professionnel et Pokémon Go. Le CERT-FR constate qu'il est « *tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capturer un Ronflex (un Pokémon rare à trouver)* ». Surtout quand la demande émane d'un VIP et qu'il est souvent difficile de refuser. Eh bien comme Patrick Pailloux (prédécesseur de Guillaume Poupard à la tête de l'ANSSI) l'avait dit en son temps, il faut avoir le pouvoir de dire non à l'installation de ce type d'application dans un environnement professionnel.

Toujours dans le cadre du travail, l'agence déconseille l'usage de l'application dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles).

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : L'ANSSI alerte sur les risques liés à Pokémon Go

Privacy Shield : 1 an de sursis donné par les CNIL européennes

	Privacy Shield : 1 an de sursis donné par les CNIL européennes

Les CNIL européennes ne sont pas satisfaites du Privacy Shield, mais prennent date en 2017 pour s'inviter dans la révision de l'accord.

Le verdict était attendu. Les CNIL européennes du groupe de l'article 29 (G29) ont rendu leur décision définitive sur le Privacy Shield. Cet accord encadre le transfert des données entre les Etats-Unis et l'Union européenne Il est le successeur du Safe Harbor, invalidé par la Cour de Justice de l'Union européenne. Dans un communiqué de presse, le G29 souligne ses réserves sur le Privacy Shield. Il considère néanmoins que l'accord a été voté et il donne rendez-vous au 1 an de l'accord lors de sa révision pour un examen plus approfondi de certaines dispositions.

En avril dernier, le groupe avait émis différentes critiques sur le Privacy Shield. Il avait souligné *« un manque de clarté général »*, une *« complexité »*, et parfois une *« incohérence »*, des documents et annexes qui composent le Privacy Shield. C'est notamment le cas pour les voies de recours que pourront emprunter les citoyens européens contestant l'exploitation de leurs données outre-Atlantique, indique le groupe dans son avis consultatif.

Quant à l'accès des agences de renseignement aux données transférées dans le cadre du Privacy Shield (volet sécurité nationale), il soulève de *« fortes préoccupations »*. Le risque d'une collecte *« massive et indiscriminée »* des données par un État n'est pas écarté. Le groupe s'inquiète aussi du statut et de l'indépendance du médiateur (*« ombudsman »*) vers lequel les citoyens européens pourront se tourner.

Un an de sursis et une mise en garde

Certaines réserves ont été prises en compte, note le G29, mais « cependant un certain nombre de préoccupations demeurent ». Au premier rang desquels, le risque toujours bien réel d'une surveillance de masse par le gouvernement américain. Il évoque le rôle du médiateur et la révision annuelle de l'accord.

Les CNIL européennes comptent beaucoup sur cette révision annuelle prévue en juillet 2017. Elles profiteront de cette occasion « *pour non seulement évaluer si les questions en suspens ont été résolues, mais aussi si les garanties prévues par le Privacy Shield entre les Etats-Unis et l'UE sont réalisées et efficaces* ». Et de prévenir, que « *tous les membres de l'équipe en charge de cette révision doivent avoir accès à toutes les informations nécessaires à l'accomplissement de leur examen y compris des éléments favorisant leur propre évaluation sur la proportionnalité et la nécessité de la collecte et l'accès aux données par les pouvoirs publics* ». Une mise en garde contre les risques d'être éconduits dans un an.

Pendant ce temps-là, le Privacy Shield pourrait être contesté par des citoyens européens, comme cela a été le cas avec Max Schrems pour le Safe Harbor. Lors d'une récente discussion dans le cadre de Cloud Confidence, le jeune avocat avais émis l'hypothèse d'une nouvelle action en justice contre le Privacy Shield.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Privacy Shield : les CNIL européennes accordent 1 an de sursis

La Cnil épingle Windows 10 sur la collecte des données personnelles

La Cnil épingle Windows 10 sur la collecte des données personnelles

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.
Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.
De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.
De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.
Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.
La balle est maintenant dans le camps de Microsoft.
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : La Cnil épingle Windows 10 sur la collecte des données

---

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

L’Arménie à son agence de protection des données à caractère personnel

L’Arménie à son agence de protection des données à caractère personnel

---

L’agence de protection des données à caractère personnel a fourni des conseils à plus de 300 organisations en 3 mois

L’Agence de protection des données personnelles, une structure affiliée au Ministère arménien de la justice a fourni des conseils à plus de 300 organismes au cours des trois derniers mois selon sa responsable Suse Doydoyan.
Elle a dit que 98% de ces organisations était des structures privées, “mais nous avons fourni des conseils également aux organisations du secteur public.“
Selon elle, l’agence a aussi fait beaucoup de travail au cours des 100 derniers jours pour étudier l’expérience internationale et a travaillé sur un certain nombre de concepts relatifs. Elle a souligné que l’agence n’est pas un organe répressif, bien que possédant des « leviers d’influence importants, y compris le pouvoir d’engager des procédures administratives.
“Nous pensons que notre fonction est préventive. Nous n’attendons pas que des violations se produisent afin d’infliger des amendes subséquentes, essayant d’abord d’empêcher ces violations“ a-t-elle dit.
L’Agence de protection des données personnelles agit au nom de la République d’Arménie.

Article original de Stéphane

Réagissez à cet article

Original de l’article mis en page : Nouvelles dArménie en Ligne

---

Privacy Shield : un « bouclier » troué à refuser !

#Privacy Shield : un « bouclier » troué à refuser !

Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette décision, adoptée dans la plus grande précipitation, ne répond pas aux inquiétudes exprimées ces dernières semaines à tour de rôle par le groupe des CNILs européennes, le Parlement européen et différents gouvernements européens, ainsi que par les associations de défense des droits.

Le 6 octobre 2015 la Cour de justice de l'Union européenne avait annulé l'accord du « Safe Harbor » couvrant les transferts de données depuis 2000, estimant que celui-ci permettait une collecte massive des données et une surveillance généralisée sans offrir de voies de recours effectives aux États-Unis pour les individus concernés en Europe. Aujourd'hui, force est de constater que le Privacy Shield ne répond pas non plus aux exigences de la Cour de justice.
Sur les principes de respect de la vie privée qui incombent aux entreprises couvertes par le Privacy Shield, on peut se demander l'utilité même d'une telle décision dans la mesure où celle-ci ne se substituera pas aux clauses contractuelles types ni aux règles internes d'entreprises, moins contraignantes et actuellement en vigueur, mais qu'elle s'y ajoutera. Cela signifie que si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations qui lui incombent en matière de vie privée, elle pourra continuer à traiter des données avec les deux mécanismes internes cités plus hauts.
Mais le cœur de la décision se retrouve plutôt dans le chapitre sur l'accès aux données par les autorités publiques des États-Unis. Dans le texte, il n'est pas question de « surveillance de masse » mais plutôt de « collecte massive ». Or, si les États-Unis ne considèrent pas la collecte de masse comme de la surveillance, l'Union européenne, elle, par l'intermédiaire de sa Cour de justice, a tranché sur cette question en considérant, dans l'affaire C-362/14 Schrems c. Data Protection Commissioner, que la collecte massive effectuée par l'administration des États-Unis était de la surveillance de masse, contraire à la Charte des droits fondamentaux de l'Union européenne. Cette décision avait mené à l'invalidation du « Safe Harbor », et tout porte à croire que les voeux pieux et les faibles garanties d'amélioration exprimées par le gouvernement américain ne suffiront pas à rendre la décision du Privacy Shield adéquate avec la jurisprudence européenne.
Il en va de même sur la question des possibilités de recours. L'une des exigences de la CJUE, des CNIL européennes, du contrôleur des données personnelles et de la société civile était que toute personne concernée par un traitement de données avec cet État tiers puisse avoir la possibilité de déposer une plainte et de contester un traitement ou une surveillance illégale. Pour pallier cette sérieuse lacune du Safe Harbor, un mécanisme de médiateur (« #Ombudsperson ») a été instauré. L'initiative aurait été bonne si ce médiateur était réellement indépendant. Mais d'une part il est nommé par le Secrétaire d'État, d'autre part les requérants ne peuvent s'adresser directement à lui et devront passer par deux strates d'autorités, nationale puis européenne. L'Ombudsperson pourra simplement répondre à la personne plaignante qu'il a procédé aux vérifications, et pourra veiller à ce qu'une surveillance injustifiée cesse, mais le plaignant n'aura pas de regard sur la réalité de la surveillance. Cette procédure ressemble à celle mise en place en France par la loi Renseignement avec la #CNCTR et, pour les mêmes raisons, ne présente pas suffisamment de garanties de recours pour les citoyens.
Le projet de Privacy Shield, préparé et imposé dans la précipitation par la Commission européenne et le département du Commerce américain, ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. Les gouvernements européens et les autorités de protection des données doivent donc absolument refuser cet accord, et travailler à une réglementation qui protège réellement les droits fondamentaux. Les nécessités d'accord juridique pour les entreprises ayant fait de l'exploitation des données personnelles leur modèle économique ne peuvent servir de justification à une braderie sordide de la vie privée de dizaines de millions d'internautes européens.
Article original de La Quadrature du Net

Réagissez à cet article

Original de l'article mis en page : Privacy Shield : un « bouclier » troué à refuser ! – Global Security Mag Online

---

Données personnelles : le

« Privacy Shield » dans la dernière ligne droite

Données personnelles : le « Privacy Shield » dans la dernière ligne droite

Le Privacy Shield (« bouclier de protection des données personnelles »), un accord politique censé encadrer l'utilisation des données personnelles des citoyens Européens par les entreprises sur le sol américain, a été validé par les Etats membres, vendredi 8 juillet.

Pour la première fois, les Etats-Unis ont donné à l'Union européenne l'assurance écrite que l'accès des autorités aux données personnelles serait soumis à des limitations claires, des garde-fous et des mécanismes de contrôle, tout en écartant la surveillance de masse indiscriminée des données des Européens » s'est réjoui la commission dans un communiqué.

Le Privacy Shield est censé remplacer le Safe Harbor, un accord similaire qui a été invalidé par la Cour de justice de l'Union européenne (CJUE), qui a notamment cité le peu de cas que faisaient les agences de renseignement américaines des données personnelles des citoyens européens stockées sur le sol américain.
Les entreprises du numérique, placées dans une situation juridiquement inconfortable depuis l'annulation du Safe Harbor, ont salué cette étape supplémentaire sur le chemin de l'adoption définitive. « Même si les négociations n'ont pas été faciles, nous félicitons la commission et le ministère du commerce américain pour leur travail de restauration de la confiance dans les transferts des données entre l'UE et les Etats-Unis », a dit John Higgins, le directeur général de DigitalEurope, un lobby rassemblant notamment Google, Apple, Microsoft et IBM, qui dit aussi espérer que grâce au Privacy Shield « l'Europe puisse à nouveau se concentrer sur la manière dont les flux de données peuvent jouer un rôle dans la croissance économique ».

DE NOMBREUX OBSTACLES DEMEURENT

L'accord, entre la commission et les Etats-Unis, doit encore être validé par le collège des commissaires européens, avant son adoption définitive qui devrait intervenir le 12 juillet prochain, après des mois d'âpres négociations. Ce n'est pas la fin du débat autour de cet accord contesté.
L'accord n'a pas fait consensus auprès des Etats membres, les diplomates représentant plusieurs pays – l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters – se sont abstenus. Un moyen d'« exprimer leur méfiance vis-à-vis du texte » anticipait, jeudi lors d'une conférence, David Martinon, ambassadeur français pour la cyberdiplomatie et l'économie numérique, cité par le site Silicon.fr.
Par ailleurs, cet accord, sera très certainement contesté devant les tribunaux après son adoption. Max Schrems, l'Autrichien tombeur du prédécesseur du Privacy Shield, pourrait attaquer l'accord devant les juridictions européennes.
Dans le même ton, La Quadrature du Net, association française de défense des libertés numériques, a dénoncé un accord qui « ne présente pas les garanties suffisantes pour la protection de la vie privée des Européens. Il passe sciemment à côté du cœur de l'arrêt de la CJUE invalidant le Safe Harbor : la surveillance massive exercée via les collectes de données des utilisateurs. »
Article original de Martin Untinsinger

Réagissez à cet article

Original de l’article mis en page : Données personnelles : le « Privacy Shield » dans la dernière ligne droite

---

Ce qui changera après l’adoption du règlement général sur la protection des données

Ce qui changera après l’adoption du règlement général sur la protection des données

---

La Cnil a mis en ligne, le 15 juin dernier, une de ses synthèse qui facilitent, même pour les juristes, lappréhension intellectuelle dune nouvelle législation, en loccurrence le désormais célèbre « Règlement général sur la protection des données », puisque tel est le nom raccourci officiel du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à légard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (notre actualité du 4 mai 2016).

À très grands traits, selon la Cnil :

« La réforme de la protection des données poursuit trois objectifs :
• Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
• Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
• Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées. »
Source : « Règlement européen sur la protection des données : ce qui change pour les professionnels », Cnil, 15 juin 2016.
S'ensuit une série de chapitres présentant les diverses facettes des quelque 173 considérants et 99 articles du règlement ainsi décrypté :
• Un cadre juridique unifié pour l'ensemble de l'UE
• Un renforcement des droits des personnes
• Une conformité basée sur la transparence et la responsabilisation
• Des responsabilités partagées et précisées
• Le cadre des transferts hors de l'Union mis à jour
• Des sanctions encadrées, graduées et renforcées
• Comment les autorités de protection se préparent-elles ?

Peu de changements en vérité…

Signalons, pour ceux qui s'imagineraient que tout change puisque le nouveau règlement abroge toutes les lois de protection des données des États membres de l'Union, que les changements sont en fait fort peu nombreux et que le cadre de protection, surtout tel que nous le connaissions depuis la réforme de notre loi du 6 janvier 1978 sous l'influence de l'ancienne directive 95/46 CE, en date du 1er août 2004. Ce sont les mêmes fondements qui ont présidé à l'élaboration de ces règles communes, automatiquement insérés dans le droit national des États membres.

…Mais des changements piégeant à la marge

Mais cependant, il faut s'attendre à des changements, d'autant plus subreptices qu'ils interviennent dans un océan de stabilité.
On pourrait distinguer deux ordres de dispositions modificatrices :
• Les dispositions qui sont réellement nouvelles, comme par exemple, en France, la disparition des déclarations préalables à la Cnil et quelques autres dispositions vraiment nouvelles ;
• Les dispositions qui existaient déjà dans l'ancienne directive mais qui n'avaient pas été transposées dans la loi d'un pays membre. C'est par exemple le cas du droit à l'oubli dans la loi allemande.

Une marge de manœuvre résiduelle

Cependant, il reste dans le règlement, une certaine latitude d'action de la part des États membres. On peut le comprendre techniquement en comparant un règlement européen à une loi nationale, ce qu'il est effectivement. Il faut donc prendre en compte le fait que chaque pays pourra selon sa sensibilité prendre les mesures d'application de ce règlement – sous forme de décrets en France – ce qui aura de nouveau pour effet d'introduire des divergences de régime d'un pays à l'autre.

Article original de Didier Frochot

Réagissez à cet article

Original de l’article mis en page : Le règlement général sur la protection des données : ce qui change en Europe

---

Que change le brexit pour la protection des données personnelles ?

Que change le brexit pour la protection des données personnelles ?

Le nouveau règlement européen sur les données personnelles, qui doit entrer en vigueur en mai 2018, ne s'appliquera peut-être jamais au Royaume-Uni. Le pays devrait, une fois sorti, conserver sa propre législation, basée sur les directives européennes antérieures. Cela pourrait obliger le Royaume-Uni à conclure un accord spécifique avec l'UE à 27, sous peine de se voir infliger des restrictions dans le transfert de données avec les pays de l'UE.

Le Royaume-Uni se retrouverait ainsi dans la même position que lesEtats-Unis, dont l'accord avec l'UE (Safe Harbor) a été remis en cause à l'automne pour être remplacé par le Privacy Shield, qui devrait entrer en vigueur cet été. L'adhésion à ces accords conditionne la possibilité de transférer des données personnelles de citoyens de l'UE aux Etats-Unis.

Si le Safe Harbor a été remis en cause, c'était notamment à cause des questions de surveillance de masse aux Etats-Unis. Soit le Royaume-Uni choisit de se rapprocher du modèle américain sur les questions de surveillance et de données personnelles, soit il se cale sur les standards européens.

Dans le premier cas, il faudrait que les grandes entreprises américaines (Google, Apple, Facebook, Microsoft…), dont la plupart des datacenters sont à Dublin, en Irlande, les rapatrient au Royaume-Uni, comme le note le site de la radio publique irlandaise RTE. La présence de ces datacenters en Irlande doit rassurer les Européens, puisque l'Irlande, elle, n'est pas concernée par le Brexit. Ce sont donc les standards européens qui s'appliquent.

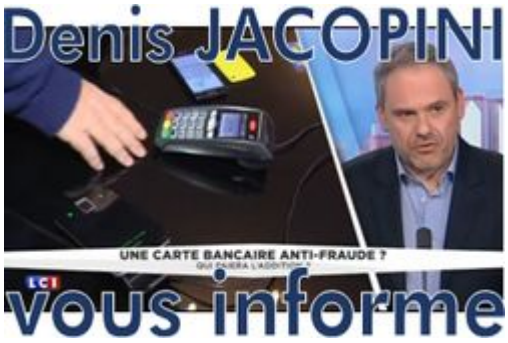
Avant la sortie effective, rien ne change. « A moyen terme, les choses vont rester très stables. Le Royaume-Uni met en oeuvre la directive européenne sur les données personnelles depuis plus de 20 ans. La suite dépendra des accords qui seront négociés entre le Royaume-Uni et l'UE. Le cadre réglementaire ne changera donc pas pendant un bon bout de temps », assure à L'Express Daniel Kadar, avocat associé au cabinet Reed Smith.

Article original de Raphaële Karayan

Réagissez à cet article

Original de l'article mis en page : Ce que le Brexit va changer pour les géants du Web – L'Express L'Expansion

L’État crée encore un nouveau fichier secret de données personnelles



L’État crée encore un nouveau fichier secret de données personnelles

Le gouvernement a fait connaître vendredi la création d'un fichier de données personnelles utilisé pour les services de renseignement intitulé « #BCR-DNRED », dont le contenu et la portée sont confidentiels. Il s'agit d'un fichier permettant les enquêtes contre la fraude douanière, orienté vers les crimes graves.

Le gouvernement a fait publier vendredi au Journal Officiel un décret n° 2016-725 du 1er juin 2016 qui ajoute un 13e fichier à la liste des fichiers confidentiels de données personnelles mis en œuvre par l'État, « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* ».
Comme le veut la règle, on ne sait strictement rien de ce fichier si ce n'est qu'il est baptisé « BCR-DNRED » et sera utilisé par les « *services du ministère des finances et des comptes publics (administration des douanes et droits indirects) traitant de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la prolifération des armes de destruction massive* ».
L'acronyme BCR-DNRED est sans aucun doute une référence à la Direction nationale du renseignement et des enquêtes douanières (DNRED), rattachée à Bercy. Considérée comme un service de renseignement, elle est chargée notamment de collecter des informations sur les les grands trafics de contrebande, et de lutter contre les flux financiers clandestins.

UN FICHIER CONTRE LE TRAFIC

JORF n°0128 du 3 juin 2016
texte n° 87

Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED »

NOR: CNIX1614799X
ELI: Non disponible

Avis favorable avec réserve.

L'avis « favorable avec réserve » de la Cnil.

On imagine donc que le fichier BCR-DNRED s'inscrit dans une politique de croisement d'informations concernant de possibles trafics internationaux illicites de biens ou d'argent qui transitent par la France, avec une orientation plus spécifique vers la recherche de financements de crimes graves.
La Cnil, qui n'a pas le droit de publier son avis, a émis un avis « favorable avec réserve », ce qui veut dire qu'elle a estimé qu'au moins sur certains points, le fichier projeté n'était pas conforme à la loi de 1978 sur la protection des données personnelles. Elle avait déjà émis des réserves non publiées concernant les deux derniers fichiers créés par l'État, le fichier CAR relatif au suivi des prisonniers créé en novembre 2015, et le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT) modifié quelques jours plus tôt.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : L'État crée encore un nouveau fichier secret de données personnelles — Politique — Numerama