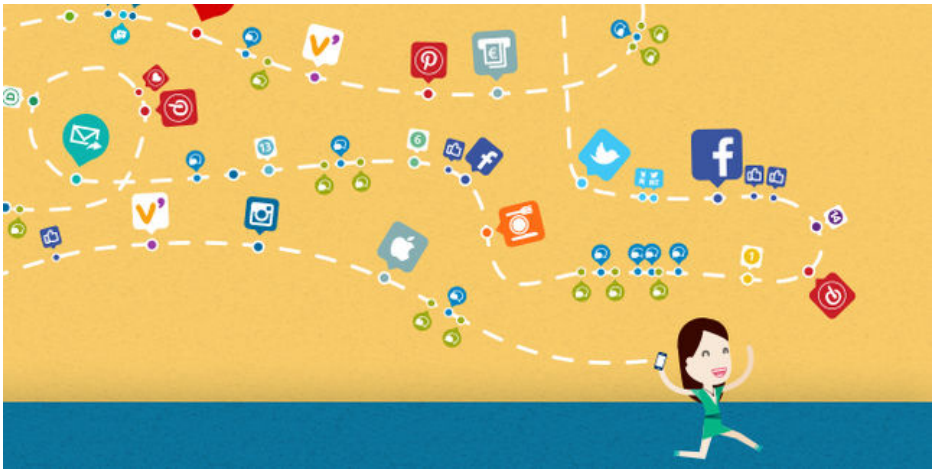
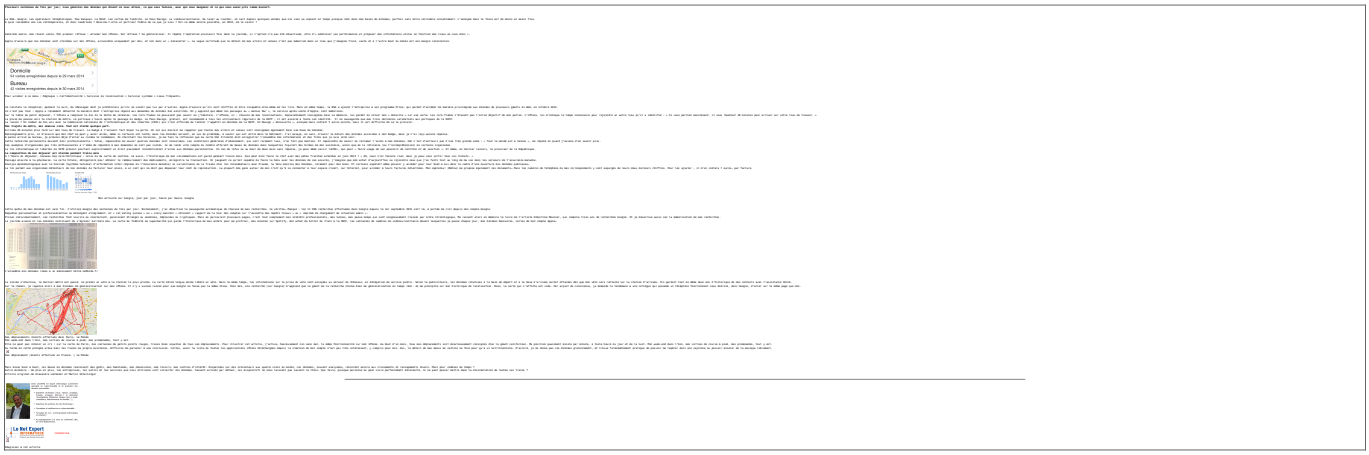
Ma vie disséquée à travers mes données personnelles



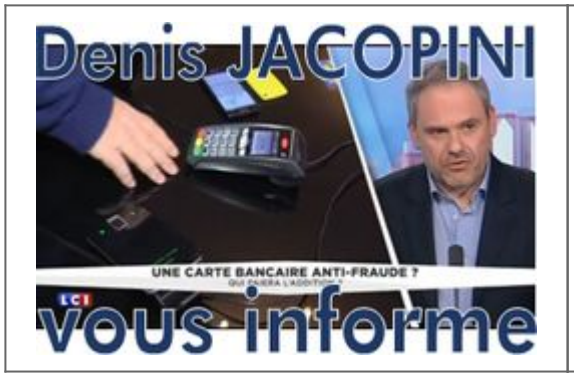
Ma vie disséquée à travers mes données personnelles



Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

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.

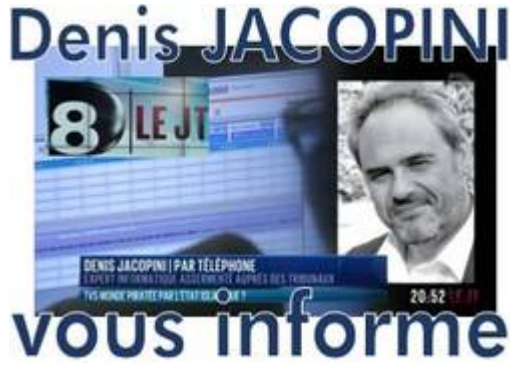
Article original de Jacques Cheminat

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

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

---

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

---

Privacy Shield : un «

bouclier » troué à refuser !

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

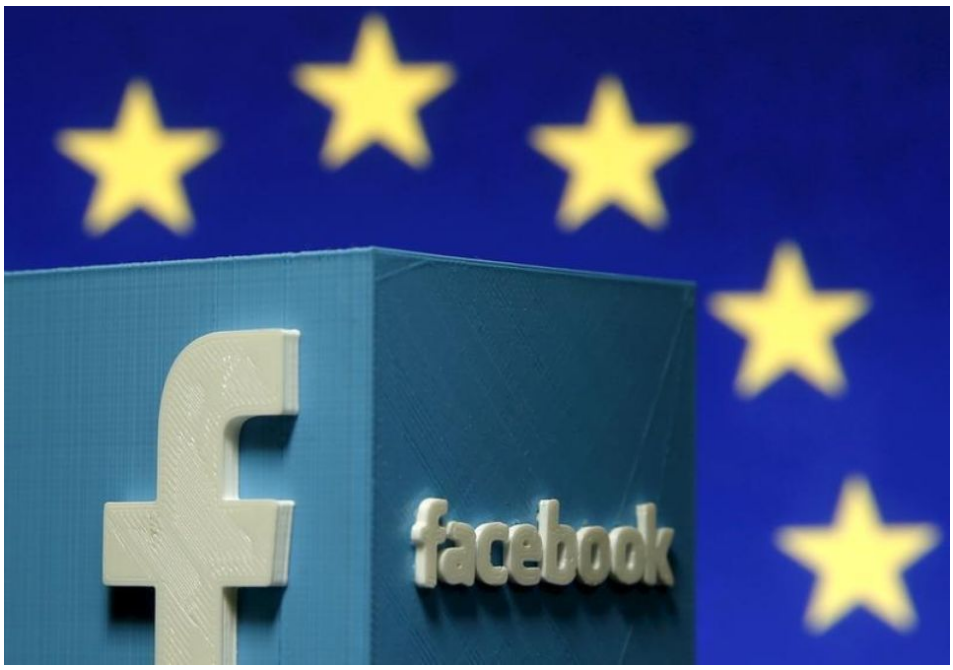
Le 8 juillet 2016, les États membres de l'Union européenne, réunis dans ce qu'on appelle le « comité de l'article 31 », se sont prononcé sur l'adoption de la décision d'adéquation qui encadrera les échanges de données personnelles entre les États-Unis et l'Union européenne : le Privacy Shield. Cette 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

L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté



L’accord entre l’Europe et les Etats-Unis sur les données personnelles sur le point d’être adopté

Les Etats membres de lUE ont donné leur feu vert au «Privacy Shield», qui vient remplacer laccord «Safe Harbor» invalidé en octobre par la justice européenne.

Le «Privacy Shield» est sur la rampe de lancement. La Commission européenne l'a annoncé ce vendredi matin : le nouvel accord-cadre sur les transferts de données personnelles depuis le Vieux Continent vers les Etats-Unis a reçu le feu vert des Etats membres de l'Union, moins quatre abstentions (l'Autriche, la Slovénie, la Bulgarie et la Croatie, selon l'agence Reuters). Il devrait être adopté formellement par la Commission mardi prochain. Ce «bouclier de confidentialité» vient ainsi succéder à l'accord dit «Safe Harbor» (ou «sphère de sécurité»), invalidé il y a neuf mois par la justice européenne.

Deux ans de négociation

Mis en place en 2000, le Safe Harbor était censé garantir aux citoyens européens un niveau de protection suffisant de leurs données personnelles transférées sur le sol américain : les entreprises qui y adhéraient s'engageaient à respecter les normes de l'UE en la matière… via une certification annuelle qu'elles pouvaient s'autodécerner. Une «garantie» minimale qui a volé en éclats en 2013 avec les révélations d'Edward Snowden sur les pratiques de surveillance massive de la NSA, et notamment le programme Prism, qui permet à l'agence américaine d'accéder aux données stockées par les géants du Net.
Article original de Amaelle Guiton
Photo Dado Ruvic. Reuters

Réagissez à cet article

Original de l’article mis en page : Données personnelles : laccord entre lEurope et les Etats-Unis sur le point dêtre adopté – Libération

---

Évolution du « Safe Harbor » vers le l’ »UE-US Privacy Shield »

Évolution du « Safe Harbor » vers le l’ »UE-US Privacy Shield »

La Commission européenne et les États-Unis ont convenu d'un nouveau cadre pour les transferts transatlantiques de données, l' « UE Privacy Shield », en lieu et place du « Safe Harbor ».

Le cadre était attendu depuis l'annulation du Safe Harbor par la Cour de justice de l'UE (CJUE) dans son arrêt du 6 octobre 2015, qui avait créé un vide juridique important en matière de transfert des données (voir notre article).
La Commission européenne et le groupe des CNIL européennes (G29) avaient, d'ailleurs, apporté une première réponse aux inquiétudes des entreprises confirmant que les clauses contractuelles types et les Binding Corporate Rules (BCR) restaient les solutions à privilégier pour assurer la conformité des transferts en cours, durant cette période de transition (voir notre brève).
Ce « bouclier de la confidentialité », présenté le 29 février dernier, aurait donc vocation à protéger les droits fondamentaux des Européens en cas de transfert des données aux États-Unis et à fournir des garanties aux entreprises qui font des affaires transatlantiques.

De nouvelles obligations pour les entreprises américaines
« La collaboration des deux partenaires de part et d'autre de l'Atlantique vise à ce que les données individuelles soient parfaitement protégées, sans renoncer pour autant aux possibilités qu'offre l'ère numérique », a déclaré Andrus Ansip, vice-président de la Commission européenne lors de la présentation publique du Privacy Shield. Et cette protection des données personnelles passerait d'abord par un encadrement des politiques des entreprises américaines en la matière. C'est en tout cas le souhait de la Commission. Le projet de « bouclier » prévoit que les entreprises américaines souhaitant importer des données personnelles provenant d'Europe devront s'engager, dans un code de bonne conduite, à respecter des conditions strictes quant à leurs traitements.
Le dispositif actuel du Privacy Shield prévoit aussi des mécanismes de surveillance afin de garantir le respect de ces obligations par les entreprises. Ces dernières seraient ainsi obligés de rendre public leurs engagements en la matière, qui restent pour le moment à définir, sous peine d'être sanctionnées par la Federal trade commission.
En cas de non-respect de ces engagements les citoyens européens pourraient déposer plainte contre les agissements des entreprises. Elles auront alors 45 jours maximum pour y répondre. Cependant, aucune sanction n'est prévue à ce jour si les délais sont dépassés. Pour que leurs plaintes soient traitées, les citoyens européens pourraient également s'adresser à leur CNIL nationale qui collaborera avec la Federal trade commission. L'instance américaine devra apporter une réponse dans les 90 jours. Enfin pour les cas non résolus, l'accord américano-européen prévoit le recours, en dernier ressort, à un tribunal d'arbitrage devant lequel les entreprises pourront être convoquées. La Commission précise que ce mécanisme de règlement extrajudiciaire des litiges sera accessible sans frais.
La surveillance des services de renseignements plus encadrée
Outre ces mécanismes de surveillance concernant les entreprises, l'exécutif européen a affirmé avoir obtenu de la part des américains un strict encadrement de l'accès des autorités publiques aux données personnelles. « Pour la première fois, le gouvernement américain, par l'intermédiaire des services du directeur du renseignement national, a donné par écrit à l'UE l'assurance que tout accès des pouvoirs publics aux données à des fin de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, empêchant un accès généralisé aux données personnelles », s'est félicité Bruxelles dans un communiqué. Selon cet engagement pris par les américains, les citoyens européens disposeront d'un recours dans le domaine du renseignement national grâce à un mécanisme de médiation indépendant des services de sécurité nationaux. A ce jour, aucune précision n'a été donné sur les conditions de nomination de ce médiateur ni aucune garantie concrète concernant son indépendance, ce que regrettent les détracteurs de ce texte.
Pour que les limitations de l'accès des pouvoirs publics soient respectés, le Privacy Shield prévoit un mécanisme de réexamen commun aux deux continents. En effet, la Commission européenne et la Federal trade commission, associés à des experts nationaux, pourraient contrôler chaque année le respect des engagements en s'appuyant sur toutes sources d'informations disponibles comme les rapports annuels de transparence des entreprises et ceux d'ONG spécialistes du respect de la vie privée. Côté européen, la Commission adressera un rapport public au Parlement européen et au Conseil, à la suite de ce réexamen.
Ce nouveau cadre international de protection des données doit encore être adopté par le collège des commissaires européens, après l'avis des autorités européennes chargées de la protection des données. En parallèle, les États-Unis vont devoir mettre en place ce nouvel instrument ainsi que les mécanismes de contrôle et de médiation. De nombreuses modifications ont encore le temps d'être apportées, surtout dans le contexte international des élections présidentielles américaines… [Lire la suite]

Réagissez à cet article

Source : *[Direction juridique] L'actualité actuEL DJ : Du « Safe Harbor » à l' »UE-US Privacy Shield »*

Safe Harbor & Privacy Shield : Comment l'entreprise peut avoir le contrôle complet de son propre cloud ?

Safe Harbor & Privacy Shield : Comment l'entreprise peut avoir le contrôle complet de son propre cloud ?

L'invalidation de l'accord Safe Harbor a provoqué une certaine incertitude chez de nombreuses entreprises qui ne savent plus comment sauvegarder leurs données en toute sécurité et légalité – tout en les mettant à la disposition de leurs collaborateurs.

Début février, l'accord Safe Harbor 2.0 – surnommé Privacy Shield – a vu le jour, mais de nombreux doutes sur sa légitimité subsistent.
Dans ce contexte, l'incertitude demeure au sein des entreprises qui se posent de nombreuses questions autour de la conformité et ne savent pas si le Privacy Shield sera une solution sur le long terme. Il est toutefois possible de contourner les problématiques liées à l'instabilité de telles réglementations en trouvant la bonne solution – ainsi qu'un fournisseur de services adapté.

Il existe deux alternatives pour sauvegarder et utiliser ses données en toute sécurité dans le cloud sans se soucier de problématiques de conformité.
D'une part, l'entreprise peut rechercher un fournisseur de cloud computing exploitant ses Data Centers dans un pays européen. D'autre part, les entreprises sont tout à fait capables de constituer leur propre cloud et d'y mettre leurs données, ressources informatiques et applications à la disposition de leurs collaborateurs. Le marché du stockage externe offre de nombreuses solutions pour ces deux approches. Le rôle, pour tous les grands acteurs sur le marché, étant d'offrir aux clients une sauvegarde et un partage parfaitement sûrs de leurs données dans le cloud.

Les utilisateurs du cloud doivent pouvoir faire entièrement confiance à leur fournisseur de services
Dès qu'une entreprise prend la décision d'utiliser une architecture cloud public pour stocker une partie de ses informations, elle doit trouver un fournisseur adapté à ses exigences mais également irréprochable en termes de fiabilité.
La priorité dans cette démarche, lorsque l'on souhaite éviter des soucis de conformité, est de s'assurer que le fournisseur mette à disposition ses centres de données en Europe. En outre, l'entreprise est parfaitement en droit de demander si la sauvegarde de données de son fournisseur est effectuée exclusivement dans ses propres centres de données ou s'il en fournit une copie à d'autres centres de données d'un pays tiers. L'évaluation des accords de niveau de service (SLA), de la méthode et de la chronologie de sauvegarde appliquée pour telles ou telles données mais aussi des conditions de leur récupération sont des points à examiner lors du choix du fournisseur.
Cela permet d'établir une solution de confiance entre l'utilisateur et son service cloud. C'est sur la base de cette confiance et de la garantie que leurs données ne quittent pas l'Europe que les utilisateurs peuvent opter pour différents services de cloud.
D'autre part, l'utilisateur doit impérativement veiller à ce que le fournisseur utilise un encodage afin d'écarter tout risque d'utilisation abusive (intentionnelle ou aléatoire) de ses données.

L'entreprise peut avoir le contrôle complet de son propre cloud
La deuxième option garantie une sauvegarde et un partage des données parfaitement sûrs dans une architecture cloud, et confère donc à l'entreprise le plein contrôle sur ses informations et services numériques. Légèrement plus complexe, cette option consiste à créer sa propre architecture cloud privée.
L'entreprise devra certes gérer davantage de ressources, mais elle pourra puiser pleinement dans les services mis à disposition, les droits d'accès, la sélection des applications et l'assistance technique. Ces avantages garantiront une meilleure flexibilité aux collaborateurs de l'entreprise, ainsi que des outils nécessaires pertinents pour faciliter leurs tâches et les mêmes droits d'utilisation que s'ils travaillaient dans un cloud public. La sécurité des données et des appareils sera également garantie conformément aux mesures internes prises par l'entreprise.
Un cloud privé n'est pas concerné par les effets de Privacy Shield et permet d'utiliser différents services basés sur le cloud computing. En effet, les applications telles que « Box » ou « Dropbox » ne devraient plus être utilisées dans un environnement influé par de telles réglementations.

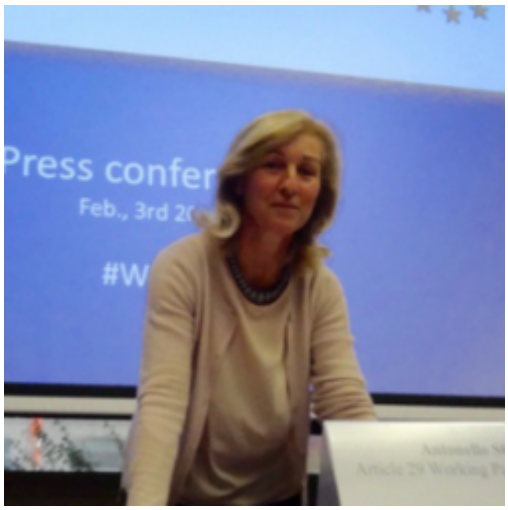
La pratique BYOD est une tendance très actuelle dans le monde de l'entreprise, mais elle complique l'intégration des terminaux dans les procédures de sauvegarde et rend difficile un contrôle complet sur toutes les informations de l'entreprise. L'utilisation combinée d'un cloud privé et de solutions d'accès, de synchronisation et de partage des fichiers est susceptible de remédier à cela. Les collaborateurs pourront ainsi accéder en toute sécurité aux données depuis n'importe quel terminal, les synchroniser et les partager avec leurs collègues, clients, partenaires et fournisseurs.
Un tel logiciel peut remplacer le serveur FTP et permet, par exemple, le libre-service en créant différents comptes utilisateurs tout en déchargeant les tâches de l'administrateur. L'intégration de solutions MDM facilite la gestion des appareils portables et assure un contrôle souple des données et des comptes.
Via l'utilisation d'une bonne solution d'accès, de synchronisation et de partage, le responsable informatique peut mettre en place une meilleure gouvernance des données en établissant des droits d'accès mais peut aussi retracer le transfert ou le partage éventuels des données concernées.
Les entreprises désireuses d'utiliser un cloud parfaitement sûr et de conserver le plein contrôle de leurs ressources et données opteront donc pour un cloud privé et des applications adaptées aux besoins de leurs collaborateurs et personnel informatique.

La sécurité doit être la priorité absolue
La débâcle provoquée par l'invalidation du Safe Harbor a permis de tirer une leçon très importante. La sécurité et la confidentialité des données doivent être des priorités absolues, quelle que soit la solution choisie par une entreprise, qu'il s'agisse d'un cloud privé ou public. Les informations numériques doivent donc impérativement être encodées avant de quitter l'entreprise ou – mieux – le réseau protégé. Une procédure de sauvegarde, par exemple, offre déjà une certaine protection, mais pour toutes les entreprises désireuses d'empêcher définitivement tout accès illicite à leurs données personnelles ou d'entreprise, l'encodage est une priorité absolue. Seul un encodage efficace est apte à garantir la protection et la sécurité des données … [Lire la suite]

Réagissez à cet article

Source : *Safe Harbor & Privacy Shield : comment assurer la conformité ? – JDN*

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données



La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données

---

La Commission Nationale de l'Informatique et des Libertés a publiquement mis en demeure Facebook de ne plus placer de cookies indésirables sur les postes des utilisateurs et d'arrêter le transfert des données personnelles de ses membres vers les Etats-Unis.

Le géant des réseaux sociaux a 3 mois pour se conformer à cette décision sous peine de sanction. La Commission Nationale de l'Informatique et des Libertés (CNIL) a ordonné à Facebook de stopper le transfert de certaines données personnelles de ses utilisateurs vers les Etats-Unis et de changer la façon dont elle récolte leurs données lorsqu'ils visitent son site web.
Dans sa mise en demeure, rendue publique lundi en fin de journée, la CNIL reproche ainsi à Facebook de transférer les données de ses membres aux Etats-Unis sur la base du Safe Harbor « ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne du 6 octobre 2015 », rappelle la commission.
La liste des griefs ne s'arrête pas là : « Le site dépose sur l'ordinateur des internautes des cookies à finalité publicitaire, sans les en avoir au préalable correctement informés ni avoir recueilli leur consentement », indique la CNIL.
Autre constat et non des moindres : « La CNIL a constaté que le site Facebook est en mesure de suivre la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte Facebook. En effet, le site dépose un cookie sur le terminal de chaque internaute qui visite une page Facebook publique, sans l'en informer. »… [Lire la suite]

Réagissez à cet article

Source : *La CNIL lance un ultimatum à Facebook au sujet des*

cookies et des transferts de données – Le Monde Informatique