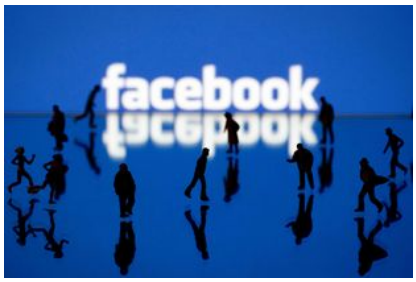
# La CNIL attaque Facebook. Que lui reproche t-elle ?




La CNIL attaque Facebook. Que lui reproche t-elle ?

**La Commission nationale informatique et liberté (CNIL), l'autorité chargée de la protection des données personnelles, a annoncé avoir mis en demeure Facebook, lundi 8 février, lui reprochant de nombreux manquements à la loi française sur la protection des données personnelles. Un long réquisitoire, contre la manière dont Facebook collecte et exploite les données de ses 30 millions d'utilisateurs français, que la CNIL a décidé de publier.**

**Que reproche-t-elle à Facebook ? La liste est longue.**

**UNE CHARGE CONTRE LA PUBLICITÉ CIBLÉE**
La CNIL estime que Facebook combine les données personnelles de ses usagers pour proposer de la publicité ciblée sans aucune base légale. Pour la CNIL, aucun consentement direct n'est donné par l'internaute, contrairement à ce qu'exige la loi française. La question de la combinaison des données personnelles en vue de la publicité est bien évoquée dans les conditions d'utilisation du réseau social, ce texte qui définit ce que peut faire ce dernier avec les données. Pour la CNIL, c'est insuffisant : la combinaison de différentes données n'est pas strictement prévue par ce « contrat » entre l'usager et le réseau social, et nécessite donc une approbation distincte de l'internaute.
La CNIL remarque que Facebook pourrait s'affranchir de ce consentement explicite en arguant, conformément à la loi, que l'affichage de publicité est fait dans l'intérêt de l'usager. Selon la CNIL, cet intérêt est trop faible et la collecte de données trop intrusive pour que Facebook se dispense d'un consentement.

**DES DONNÉES COLLECTÉES TROP SENSIBLES**
Dans certains cas, Facebook réclame des copies de documents permettant d'identifier l'utilisateur (afin, notamment, d'éviter qu'il se fasse passer pour quelqu'un d'autre). Parmi ces pièces, l'internaute peut soumettre un dossier médical : la CNIL estime que ce document est trop sensible et que le réseau social ne doit plus l'accepter.
Tout utilisateur de Facebook peut aussi renseigner, sur son profil, sa sympathie politique et ses préférences sexuelles. La CNIL juge que pour se conformer à la loi, Facebook devrait indiquer précisément ce qu'il compte faire de ces informations, compte tenu de leur sensibilité et de leur nature particulière que leur confère la loi française.

**UN MANQUE DE TRANSPARENCE**
La CNIL critique aussi vertement la manière dont Facebook explique à ses utilisateurs ce qui va être fait de leurs données personnelles. Pour la Commission, il faudrait que le réseau social les informe clairement dès le formulaire d'inscription à Facebook, conformément aux textes français, et non pas dans un texte séparé.
La CNIL juge aussi que les utilisateurs de Facebook ne sont pas suffisamment informés sur le fait que leurs données sont transférées aux USA.

**UTILISATION ILLICITE DU SAFE HARBOR**
Au sujet du transfert des données vers les Etats-Unis, la CNIL reproche aussi à Facebook de s'appuyer sur l'accord Safe Harbor. Ce dernier prévoyait que les données puissent librement être transférées, par des entreprisescomme Facebook, vers les Etats-Unis, au motif que ce pays apportait des garanties suffisantes en matière de protection des données. En octobre, la Cour de justice de l'Union européenne en a décidé autrement et l'a invalidé, au motif notamment que les Etats-Unis ne protégeaient pas suffisamment les données des Européens. La CNIL demande donc à Facebook de cesser de se baser sur cet accord pour transférer de l'autre côté de l'Atlantique les données de ses utilisateurs français.

**PROBLÈMES DE COOKIES**
Comme son homologue belge et la justice de Bruxelles avant elle, la CNIL reproche à Facebook son utilisation du cookie « datr ».
Lire aussi : La Belgique ordonne à Facebook de cesser de tracer les internautes non membres
Un cookie est un fichier qui peut être stocké sur l'ordinateur ou le téléphone d'un internaute lorsqu'il visite un site Web : il sert à mémoriser certaines informations (comme un mot de passe par exemple) ou à le reconnaître lorsqu'il visite à nouveau le même site. Facebook dépose le cookie « datr » y compris sur les appareils d'internautes qui n'ont pas de compte Facebook, lorsque ces derniers se rendent sur des pages Facebook accessibles à tous. De plus, le cookie mémorise toutes les visites de l'internaute sur les pages Web dotées par exemple du bouton « J'aime », soit la majeure partie des sites Web communément visités par les internautes français.
Facebook a fait valoir auprès la CNIL les mêmes arguments qu'il avait opposés aux autorités belges : ce cookie est destiné à reconnaître les utilisateurs « normaux » de Facebook — pour notamment empêcher le spam ou la création massive de compte — et aucun « pistage » des internautes non-inscrits à Facebook n'est effectué. Pour la CNIL, cette raison, valable, n'est pas suffisante : elle réclame à Facebook de mieux informer les utilisateurs de l'utilisation de ce cookie et des données qu'il mémorise.
La CNIL reproche aussi à Facebook de stocker trop longtemps les adresses IP — un numéro qui identifie la connexion utilisée par l'internaute pour se connecter à Internet — de ses utilisateurs.
La Commission, dans sa mise en demeure, fait de la loi de 1978 sur les données personnelles une lecture très littérale. Elle estime par exemple que Facebook y déroge en ne réclamant pas à ses utilisateurs, lorsqu'il s'inscrit, de mot de passe suffisamment compliqué. La Commission pointe qu'elle a pu s'inscrire sur le réseau social avec le mot de passe « 123456a », particulièrement faible car facile à deviner. Pour la Commission la loi impose à Facebook de prendre toutes les mesures pour protéger les données de ses membres, y compris, donc, en réclamant des mots de passe sûrs. Cette application pointilleuse devrait inquiéter de nombreuses entreprises du Web dont les pratiques sont similaires à celle du plus grand réseau social du monde.
Le réseau social dispose désormais de trois mois pour pallier les manquements repérés par la CNIL, ou demander une extension de ce délai. À l'issue de cette période, la CNIL pourra, si elle estime que Facebook n'a pas suffisamment modifié ses pratiques, entamer une procédure de sanction. … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le virulent réquisitoire de la CNIL contre Facebook*

---

# Privacy Shield : attente des détails


#Privacy Shield : attente des détails

---

**Le groupe de l'article 29 a accueilli favorablement la conclusion de l'accord « EU-US Privacy Shield ».**

Cependant, en dépit des efforts réalisés par les Etats-Unis, il réitère ses préoccupations concernant les nécessaires garanties à apporter.
Ainsi, dans son communiqué de presse en date du 3 février 2016 (1), le groupe de travail de l'article 29 rappelle, sur le fondement de la jurisprudence européenne, que quatre garanties essentielles devront être apportées pour encadrer notamment les activités de renseignement, à savoir que :
• le traitement doit être fondé sur des règles claires, précises et accessibles, de telle sorte que toute personne raisonnablement informée puisse savoir comment ses données sont traitées en cas de transfert ;
• un juste équilibre doit être trouvé entre les finalités pour lesquelles les données sont collectées et traitées et les droits des individus ;
• un système indépendant doit être mis en place pour assurer de manière effective et impartiale les contrôles nécessaires ;
• des voies de recours devant des juridictions indépendantes doivent être créées.

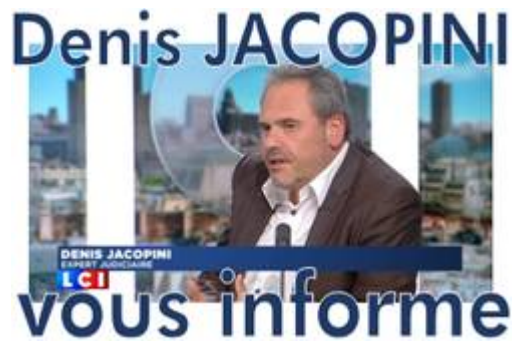
Le groupe de l'article 29 est dans l'attente de recevoir l'intégralité de la documentation du « Privacy Shield » afin de pouvoir analyser en détail son contenu.
Le groupe de l'article 29 appréciera alors si le Privacy Shield peut apporter les garanties nécessaires pour assurer un niveau de protection adéquat des données à caractère personnel, niveau qui n'est plus assuré par le Safe Harbor et a été remis en cause dans le cadre de l'affaire Schrems.
En particulier, le groupe de l'article 29 va apprécier dans quelle mesure ce nouvel accord va apporter des réponses quant à la validité des autres mécanismes de transfert.
Le groupe de l'article 29 appelle donc la Commission à lui communiquer tous les documents relatifs au « Privacy Shield » d'ici la fin du mois de février. Il sera alors en mesure de finaliser son analyse des transferts de données vers les Etats-Unis, à l'occasion d'une assemblée plénière qui sera organisée dans les semaines à venir.
A l'issue de ce délai, le groupe de l'article 29 se prononcera sur le sort des Clauses contractuelles types et des Règles Internes d'Entreprise. Dans cette attente, le groupe de travail de l'article 29 considère … [Lire la suite]

---

Réagissez à cet article

Source : *Le groupe de l'article 29 attend la communication du Privacy Shield*

# Transfert de données personnelles entre l’UE et les Etats-Unis : Accord politique trouvé




Transfert de données personnelles entre l’UE et les Etats-Unis : Accord politique trouvé

**Bruxelles – L'UE et les Etats-Unis sont parvenus la semaine dernière à un « accord politique » censé mettre fin à l'insécurité juridique dans laquelle sont plongées depuis des mois les entreprises transférant des données personnelles de l'Europe vers les Etats-Unis.**

Fruit d' »intenses négociations », le nouveau cadre annoncé mardi par la Commission européenne est destiné aux transferts transatlantiques de données personnelles entre entreprises, et doit remplacer celui qui a été invalidé en octobre dernier par la justice européenne.
Salué par les milieux économiques concernés, l'accord a cependant déjà fait l'objet de vives critiques, notamment de députés européens doutant de sa portée juridique.

Dans un arrêt retentissant concernant le réseau social Facebook mais de portée générale la Cour de justice de l'UE avait exigé de meilleures garanties pour la confidentialité des données des Européens sur le sol américain.

Les données personnelles en question englobent toutes les informations permettant d'identifier un individu, de manière directe (nom, prénom ou photo) ou indirecte (numéro de sécurité sociale ou même numéro de client).

**Nouveau « bouclier »**
Les précédentes règles, connues sous le nom de « Safe Harbor », régissaient depuis quinze ans les transferts transatlantiques de données. Sa remise en cause a provoqué un séisme pour des milliers d'entreprises, des géants comme Facebook aux nombreuses petites et moyennes entreprises traitant aux Etats-Unis des données recueillies en Europe.
Depuis plusieurs mois, elles attendaient un cadre juridique de substitution, que la Commission européenne, plutôt que « Safe Harbor 2 », a préféré rebaptiser mardi « Bouclier de confidentialité UE-USA ».

Il protégera les « droits fondamentaux » des Européens, a assuré la commissaire européenne chargée de la Justice, Vera Jourova, et donnera aux entreprises « la sécurité juridique dont elles ont besoin », a appuyé son collègue Andrus Ansip, responsable du numérique, lors d'une conférence de presse à Strasbourg.
Pour répondre aux demandes de la justice européenne, l'exécutif bruxellois a assuré que ce nouveau système serait « vivant », avec des révisions annuelles, alors que « Safe Harbor » avait fait l'objet d'un accord unique en 2000.
« Pour la première fois, les Etats-Unis ont donné à l'UE des garanties contraignantes que l'accès » aux données des Européens par les autorités américaines « feront l'objet de limites claires, de garde-fous et de mécanismes de supervision », a assuré la Commission.

Un « ombudsman » (médiateur) sera établi au sein du Département d'Etat américain, pour suivre les éventuelles plaintes et requêtes de citoyens européens concernant un accès à leurs données pour des questions de sécurité nationale.

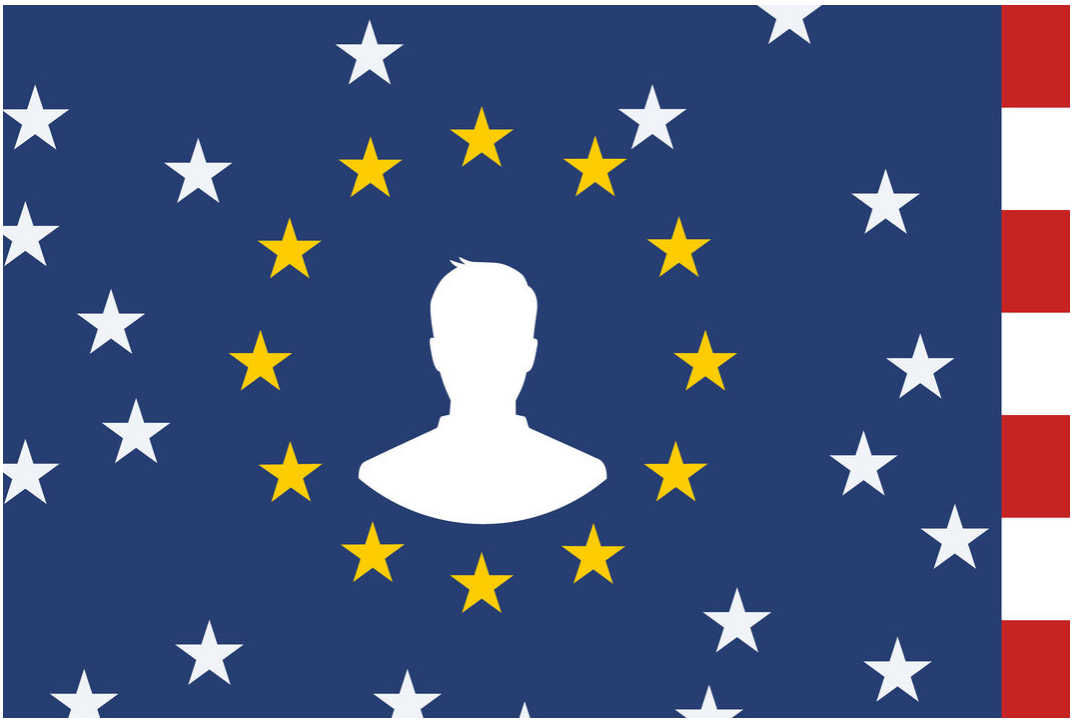
---

Réagissez à cet article

Source : *Transferts de données personnelles: « Accord politique » entre l'UE et les Etats-Unis – L'Express*

---

# Safe Harbor 2 au point mort



#Safe Harbor 2 au point mort

**A partir du 1er février, les sociétés privées transférant des données de citoyens européens vers les Etats-Unis sous le régime du « Safe Harbor » seront en infraction caractérisée. Ces sociétés bénéficiaient en effet d'une période de grâce, après l'annulation de cet accord international – mais la situation n'est toujours pas réglée.**
Pendant quinze ans, « Safe Harbor » a permis à plus de quatre mille entreprises d'exporter des données vers les Etats-Unis, alors que les lois américaines n'offrent pas une protection suffisante au regard du droit européen.
Ce régime d'exception permanente a été aboli par la cour de justice de l'Union européenne (UE) en octobre 2015, à la suite d'une plainte déposée par un militant autrichien contre la filiale européenne de Facebook en Irlande, et aux révélations d'Edward Snowden sur les programmes de surveillance de masse des agences de renseignement américaines.

**Blocage des négociations**
Malgré l'urgence, les négociations pour la mise en place d'un Safe Harbor 2, qui serait plus respectueux des droits des Européens, n'ont pas encore abouti. L'une des exigences de l'UE est que les Etats-Unis autorisent les Européens à porter plainte devant les tribunaux américains au cas où leurs données personnelles seraient exploitées de façon abusive – une simple mesure de réciprocité, car les Américains possèdent déjà ce droit en Europe. Pour satisfaire cette demande, la Chambre des représentants américaine a voté en octobre 2015 une loi spéciale, baptisée Judicial Redress Act (JRA). Le Sénat aurait dû en faire autant le 20 janvier, mais le débat a été annulé au dernier moment, sans explications.
Ce blocage affecte aussi la mise en place d'un autre accord transatlantique, conclu en septembre 2015 : l'Umbrella Agreement (« accord parapluie »), qui encadre les échanges de données personnelles en matière de police et de justice, en limitant les droits des administrations américaines dans le traitement des données européennes. Tant que le JRA ne sera pas voté, l'Europe ne souhaite pas valider l'Umbrella Agreement.

**Une loi attaquée de tous les côtés**
En réalité, aux Etats-Unis, le JRA est attaqué de tous les côtés. D'une part, certains sénateurs conservateurs, suivant l'avis des agences de renseignement, estiment que les demandes européennes arrivent à contretemps : après les attentats de Paris, la lutte contre le terrorisme exige selon eux de renforcer la surveillance des données personnelles et d'allonger leur durée de rétention, et non pas de les réduire.
D'autre part, l'association américaine de défense des libertés sur Internet, l'Electronic Privacy Information Center (EPIC), estime au contraire que l'Umbrella Agreement ne protège pas assez les données des Européens, et exige que le département fédéral de la justice publie l'intégralité du texte de l'accord, pour s'assurer qu'il ne contient pas de clauses secrètes. EPIC a écrit aux sénateurs pour les inciter à voter contre le JRA dans sa version actuelle.
Le Safe Harbor 2 semble donc mal parti, du moins à court terme, sauf si l'Europe cède à nouveau aux exigences américaines. En coulisses, à Bruxelles et dans plusieurs capitales européennes, les grandes entreprises américaines et leurs associations professionnelles font un lobbying intense pour pousser l'Union européenne a accepter un nouvel accord, même si toutes ses demandes ne sont pas satisfaites.

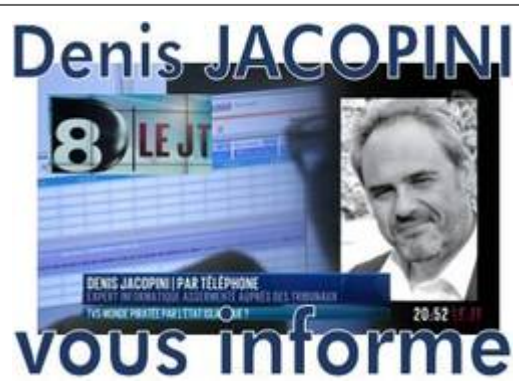
**Contrats bilatéraux pour contourner la loi**
Le groupe de travail G29, qui regroupe les agences de protection de données européennes, doit se réunir le 2 février pour évaluer la situation et si possible proposer des solutions pour sortir de l'impasse.
Les entreprises fortement impliquées dans l'exportation de données sont parallèlement déjà en train de s'adapter. Selon le cabinet juridique américain Jones Day, qui possède un bureau à Paris, la situation actuelle est incertaine, mais pas aussi critique qu'on pourrait le croire. Pour rester dans la légalité, de nombreuses sociétés ont recours à un autre instrument juridique : un contrat bilatéral entre l'expéditeur et le destinataire des données (souvent la maison-mère américaine et sa filiale européenne) contenant des clauses types garantissant que les données européennes bénéficieront aux Etats-Unis d'une protection conforme au droit européen – une procédure plus complexe et plus coûteuse que le Safe Harbor, mais pas insurmontable.
En ce qui concerne les PME européennes qui font traiter leurs données aux Etats-Unis, elles sont prises en charge par leurs fournisseurs de service, c'est-à-dire les grandes entreprises de cloud américaines comme Amazon, Salesforce ou IBM, qui se chargent à leur place des formalités juridiques.

---

Réagissez à cet article

Source : *Données personnelles : le projet « Safe Harbor 2 » dans l'impasse*

# Fic 2016 : l'avenir du Safe Harbor fixé début février




Fic 2016 : l'avenir du Safe Harbor fixé début février

**Lundi 25 Janvier, en fin de journée à Lille, lors d'une conférence plénière organisée au sein du FIC 2016, Isabelle Falque-Pierrotin a indiqué d'autre part que le G29 se réunirait début février pour savoir ce qu'il adviendra de l'annulation du Safe Harbor.**

Si la présidente de la CNIL a été discrète sur le sujet, plusieurs pistes se dégagent selon nos sources. Les clauses types et les Binding Corporate Rules (ou BCR), à savoir les codes de conduite internes aux entreprises, pourraient ne pas perdurer, sans doute parce qu'elles ne rabotent en rien la curiosité des services américains. Au-delà des autorisations individuelles, la seule issue disponible pour les acteurs du Web resterait finalement les décisions d'adéquation. Avec elle, dans un État déterminé, une autorité de contrôle devrait ainsi mener une analyse approfondie des lois nationales du pays tiers pour autoriser ou interdire le transfert.
Bien entendu, une telle position pourrait être jugée inutile si les États-Unis et l'Europe parvenaient finalement à un accord sur un hypothétique #Safe Harbor 2. Sur le terrain politique, cependant, cette réalité n'est qu'un rêve encore trop lointain. Toujours au FIC, David Martinon, représentant spécial de la France pour les négociations internationales sur la société de l'information et l'économie numérique, a pointé aujourd'hui encore l'absence d'accord entre les différents pays européens sur ce dossier.

---

Réagissez à cet article

Source : *Données personnelles : l'avenir du Safe Harbor fixé début février*

---

# Les entreprises françaises bientôt condamnées à changer leur système de traitement des donnée personnelles ?

| | |
|---|---|
|  | Les entreprises Françaises bientôt condamnées à modifier leur système de traitement des données personnelles ? |

---

**L’échéance se rapproche dangereusement. A partir de la fin du mois de janvier, entreprises américaines et européennes ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.**
Le 6 octobre 2015, la Cour de justice européenne a en effet rendu une décision invalidant le « Safe Harbor », ce traité transatlantique sur le transfert des données personnelles. Premiers touchés, les géants américains du numérique, comme Facebook, Google ou Microsoft, qui exploitent massivement les donnes personnelles.
Qu’en est-il des entreprises françaises qui, sans toujours le savoir, communiquent les données personnelles de leurs clients. De leurs salariés, de leurs contacts… sur des serveurs aux États Unis ? (Gmail, DropBox, Google Drive…)
A partir de la fin du mois de janvier, les entreprises américaines et européennes, et donc françaises, ne pourront plus faire circuler de données de part et d’autre de l’Atlantique.
Vous avez des doutes, vous souhaitez être accompagné ?
contactez-nous

---

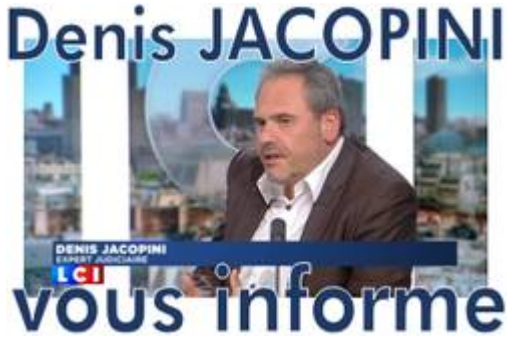
Réagissez à cet article

Source : *Fin du « Safe Harbor » : Gattaz tire la sonnette d’alarme*

---

# Des règles désormais plus

# strictes pour la protection des données privées




## Des règles désormais plus strictes pour la protection des données privées

**La réforme décidée par le Parlement, la Commission et le Conseil européen aura de profondes implications. De plus le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?**

Après 3 ans, Parlement, Commission et Conseil Européen, le « trilogue » bruxellois, sont d'accord sur la réforme de la protection de la vie privée. La directive de 1995 et ses mises à jour étaient obsolètes et furent transposés sans harmonie dans les Etats, d'où l'idée d'un règlement qui s'appliquera tout de suite.

Ce règlement s'applique aux données privées traitées, pas celle qui sont stockées en vrac. Ce sont les résultats qu'on tire de l'exploitation de ces données qui sont dangereuses. Le règlement ne s'appliquera pas aux traitements des données dans un cadre privé (ouf !). Les autorités judiciaires ne seront pas soumises au contrôle des commissions de vie privée

Celui qui gère et traite vos données (le data controller) devra bien être identifié et réel. Celui qui héberge ses données (data processor) tombe aussi sous le règlement : s'il n'est pas établi dans l'Union, le règlement s'applique à lui quand même , surtout s'il s'agit de profiler le comportement en ligne des citoyens européens. Le pays superviseur sera celui du pays du siège principal du data controller et non pas là où les data centers ont été (dé)localisés. C'est à ce prix qu'un Amazon ou Google n'aura plus à dépendre de 28 commissions de vie privée différentes. Si l'entité n'est pas présente dans l'Union, elle doit mandater un représentant.
Le règlement évoque la pseudonymisation, une contraction d'anonymisation et pseudonyme : l'usage de pseudonymes n'exempte pas les sites d'appliquer le règlement, car on peut souvent remonter à qui est derrière. Par contre, le règlement ne s'applique plus après un décès !

**Consentement**
Le consentement de l'individu au traitement de ses données, qui existe depuis 1995, sera explicite et non tacite). Le data controller doit en garder la preuve: elle sera non valable si l'utilisateur final a subi un petit chantage (par ex. un service dégradé sans ces données privées). Pour la recherche scientifique, on admet qu'il n'est pas facile de demander à l'avance ce consentement, car on ne sait pas toujours ce qui va en sortir.
Si le data controller détecte des crimes ou des menaces à l'ordre public, il doit les communiquer aux autorités. Idem en cas de cybermenace.
Si le traitement des données vise un but humanitaire, de santé publique (épidémies), ou un cas d'urgence pour l'utilisateur final, leur traitement va de soi, consentement ou pas!
Les données sur l'emploi, la protection sociale et les revenus devraient aussi pouvoir être exploitées si le but est, pour l'État, d'augmenter le bien-être public et une politique ad hoc.
Le traitement de données personnelles doit être proportionnel : si on peut l'éviter à service équivalent, c'est mieux. De même, si la société qui a des données de vous ne sait pas vous identifier, elle ne doit pas chercher à le savoir pour… avoir votre consentement.

**Les données sensibles : race, religion, opinion politique**
Les données liées à l'exercice de droits et de choix fondamentaux, comme la religion, l'appartenance politique ou la race bénéficient d'une protection renforcée. Leur traitement devrait être une exception et soumis, avant leur exécution, à une analyse d'impact du risque encouru d'un tel profilage. Par contre, les photographies ne seront pas protégées saut à contenir des données biométriques.

**Accès et rectification de données chez les tiers**
Le droit à la rectification doit être aisé à exercer, en ligne par exemple si les données ont été collectées ainsi. Une réponse, oui ou non, sera fournie dans le mois.
À charge pour le data controller de vérifier que celui qui adresse sa demande d'accès est la bonne personne. Le droit à l'oubli à la «Google» devient… un droit à l'effacement si les données collectées ne sont plus nécessaires ou ne sont plus traitées. Ce droit à l'effacement s'opérera en cascade : les entités qui auraient rendu les données publiques seront obligées d'informer les autres qui les exploiteraient ou les auraient copiés.
À une demande d'une copie de ses données personnelles (droit d'accès), c'est un format lisible par un humain qui est exigé, pas du binaire ! D'ailleurs, dit le règlement, ne faudrait-il pas un format de donnes interopérables pour permettre, enfin, la portabilité des données entre sociétés. Il n'est pas précisé si c'est applicable au cloud (car c'est du stockage, pas du traitement). Le règlement évoque les algorithmes qui prennent des décisions sur base des données personnelles ainsi que le profilage.

**Fuites et vol des données**
Les fuites de données devront être notifiées aux autorités et aux personnes impactées dans les 72 heures à moins que leur chiffrage ne les rendent inviolables. À noter tout de même un relâchement de l'obligation de notifier à la commission de vie privée tous les traitements des données personnelles, uniquement les cas risqués d'atteintes aux droits et libertés fondamentales.

**Échanges internationaux**
Les données peuvent être échangées avec des pays tiers en dehors de l'Union : c'est à la Commission de statuer si le pays répond ou non aux exigences minimales de sécurité. La Commission peut aussi retirer son agrément.
Le data controller peut toutefois continuer à opérer avec un pays « peu sûr » s'il compense avec des mesures de sécurité supplémentaires. Les sociétés peuvent mettre en place entre leurs filiales des règles internes pour atteindre un même niveau de sécurité que le règlement. Attention aux échanges avec des pays tiers (ex : les USA à la demande d'une cour) et donc à l'application extraterritoriale de ses lois à des citoyens européens : ils sont autorisés s'ils sont couverts par un traité d'assistance mutuel.
Le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

---

Réagissez à cet article

Source : *Serrage de vis européen sur la protection des données privées – Le Temps*

---

# Données personnelles –

# L’Union européenne tient son règlement


## Données personnelles – L’Union européenne tient son règlement

**Il aura fallu 3 ans de discussions et même si quelques détails restent à formaliser, tout le monde est d'accord sur le Règlement européen sur les données personnelles.**

Il aura fallu 3 ans de discussions et même si quelques détails restent à formaliser, tout le monde est d'accord sur le Règlement européen sur les données personnelles. Le Parlement, le Conseil et la Commission ont mis fin à leurs discussions en « trilogue », étape habituelle de construction d'un cadre législatif à l'échelle européenne. Ce texte très attendu entrera en vigueur au 1er janvier 2018. Il remplacera enfin la réglementation obsolète et disparate qui régit actuellement la vie privée des consommateurs de 28 pays européens. En voici les principales mesures.

**Données personnelles – : L'Union européenne tient son règlement**

L'Europe va enfin disposer d'un cadre réglementaire adapté à l'ère du numérique pour les données personnelles de ses citoyens. En clôturant leurs discussions, le 15 décembre, le Parlement, le Conseil et la Commission ont validé un texte dont les prémisses remontent à 2012. Finalement, leur version varie d'ailleurs assez peu de celle adoptée par le Parlement européen il y a 2 ans. Le nouveau règlement européen renforce la protection de la vie privée, ce dont L'UFC-Que Choisir se réjouit.

Les nouvelles règles, qui s'appliqueront au 1er janvier 2018, permettront à chacun de mieux maîtriser ses données personnelles. Concrètement, elles contraindront les sites Internet à informer très clairement les consommateurs sur la collecte et le traitement de leurs données, ce qu'ils devront expressément accepter. Le nouveau règlement définit par ailleurs un droit à la portabilité des données : il sera plus facile de transférer les données personnelles d'un prestataire de services à un autre. Par exemple, si vous passez d'Outlook à Gmail, vous pourrez rapatrier simplement vos messages, vos contacts et tous vos fichiers stockés dans le cloud. Pratique.

Précisons que sur ces deux points, le texte européen va plus loin que la loi (française) pour une République numérique, qui sera débattue au Parlement début 2016.

**Du droit à l'oubli au droit au déréférencement**

Autre mesure importante, le renforcement du droit à l'oubli numérique : si vous le demandez, et si aucun motif légitime ne s'y oppose, Google ne pourra plus indexer dans son moteur de recherche les pages Internet qui vous concernent. Petite subtilité : cela ne contraint pas les sites Internet à supprimer ces pages, c'est pourquoi il est plus juste de parler d'un « droit au déréférencement ». Cette mesure entérine une récente décision de la CJUE (Cour de justice de l'Union européenne), qui avait fait jurisprudence en la matière (lire aussi notre enquête Droit à l'oubli : Google seul juge).

Le Règlement européen valide une autre décision récente de la CJUE, qui a fait beaucoup de bruit au mois d'octobre dernier en invalidant l'accord du Safe Harbor. C'est désormais acté, les entreprises établies hors d'Europe devront se conformer à la réglementation européenne pour pouvoir offrir leurs services dans l'Union : Facebook ne pourra plus se cacher derrière ses bureaux américains pour exploiter comme bon lui semble les données de ses abonnés français ou italiens. Toute comme lui, les autres géants du Net devront en outre héberger en Europe les données des consommateurs européens.

Gare aux entreprises, européennes ou pas, qui manqueraient à leurs nouvelles obligations : le règlement prévoit des sanctions financières importantes (les montants exacts devront attendre le texte définitif, mais selon toute vraisemblance elles pourront atteindre 200 000 000 € ou 4 % du chiffre d'affaires mondial annuel d'une entreprise).

Le texte définitif doit encore être formellement adopté par le Parlement européen et le Conseil début 2016.

---

Réagissez à cet article

Source : *Données personnelles – L'Union européenne tient son règlement – UFC Que Choisir*

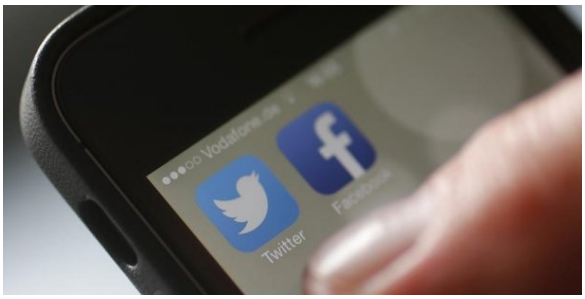
---

# L'UE parvient à un accord de principe sur la protection des données personnelles


L'UE parvient à un accord de principe sur la protection des données personnelles

---

**Les États membres conservent toutefois à leur charge la question de déterminer l'âge minimum requis pour les mineurs sur les réseaux sociaux.**




Après quatre ans d'âpres discussions, un accord de principe a finalement été trouvé mardi 15 décembre à Bruxelles, afin d'adapter la législation européenne sur la question de la protection des données personnelles à l'heure d'internet. Le texte a été validé à l'occasion d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.
« L'UE aura désormais la législation la plus étendue de protection des données personnelles dans le monde », s'est réjouie l'eurodéputée Sophie in 't Veld (libérale). L'accord prend en compte la décision récente de la justice européenne qui a déclaré « invalide » le cadre juridique qui couvre le transfert par Facebook de données personnelles de l'UE vers les Etats-Unis, a-t-elle souligné.

**Des entreprises inquiètes des sanctions**

L'accord tente de faire la synthèse entre l'exigence de donner plus de moyens de contrôle aux citoyens quant à leurs informations personnelles et la nécessité d'harmoniser les législations des États membres afin de faciliter le travail des entreprises.
Parmi les autres points de discussion, figurait notamment le montant des amendes que devront payer les entreprises qui violent les règles européennes sur la protection des données. Au terme de l'accord, les géants d'internet pourraient se voir sanctionner à hauteur de 4% de leur chiffre d'affaires annuel mondial.
Quel âge minimum sur les réseaux sociaux?
Selon cet accord, les États membres pourront fixer librement « entre 13 et 16 ans » l'âge auquel un mineur peut s'inscrire sur des réseaux sociaux comme Facebook ou Snapchat, sans l'accord d'un parent, a indiqué l'Allemand Jan-Philipp Albrecht (Verts), rapporteur du Parlement européen sur la réglementation de la protection des données.
« Malheureusement, les États membres n'ont pas pu se mettre d'accord pour fixer une limite d'âge à 13 ans pour le consentement parental à l'utilisation de réseaux sociaux comme Facebook ou Instagram », a expliqué Jan-Philipp Albrecht, à l'issue d'une réunion associant le Parlement européen, la Commission et le Conseil, qui représente les Etats.
Le Parlement européen voulait fixer cette limite à 13 ans, soit l'âge minimum requis indiqué par Facebook, mais certains Etats membres s'y sont opposés.

**Un accord contraignant**

L'accord devra encore être confirmé par le Conseil européen et voté par le Parlement au début de l'année 2016. Il restera ensuite deux ans aux États membres pour le faire entrer en vigueur. L'accord, qui comprend un règlement et une directive, a vocation à s'imposer à tous les États membres.
En juin, les ministres européens de la Justice avaient déjà trouvé un accord sur la création d'un « guichet unique » compétent pour veiller à l'application des règles pour les transferts transfrontaliers de données personnelles collectées dans plusieurs pays de l'UE par des entreprises ou des plateformes internet comme Amazon, Google et Facebook.

---

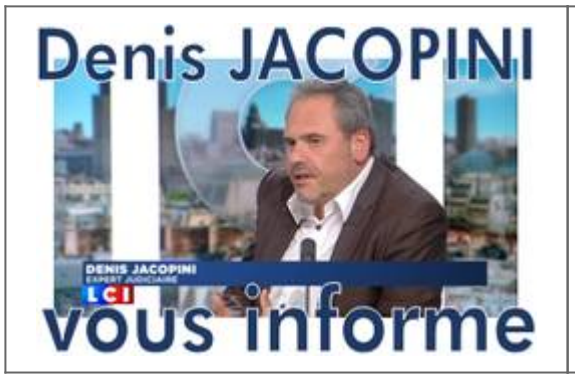
Réagissez à cet article

Source : *Protection des données personnelles: l'UE parvient à un accord de principe*

---

# Safe Harbor : les CNIL

# européennes doivent choisir entre force ou faiblesse




## Safe Harbor : les CNIL européennes doivent choisir entre force ou faiblesse

**Sans base légale mais en acceptant de prendre « un risque », les CNIL européennes ont donné jusqu'à fin janvier à l'Union européenne et aux États-Unis pour s'accorder sur un autre cadre permettant l'export de données personnelles vers les USA. Mais l'ultimatum ne sera visiblement pas respecté, et les autorités administratives hésitent sur l'attitude à adopter, entre diplomatie, force ou faiblesse.**

C'est dans une position délicate que la Cour de justice de l'Union européenne (CJUE) a plongé la CNIL et ses homologues du G29, lorsqu'elle a décidé le 6 octobre dernier d'invalider le Safe Harbor, qui permettait aux entreprises américaines comme Facebook d'importer chez elles les données des internautes européens. La plus haute juridiction de l'Union a de fait obligé les autorités de protection des données à choisir entre leur mission officielle de protection de la vie privée des citoyens, et leur contrainte officieuse de ne pas bloquer l'activité économique liée à l'exploitation des données personnelles.
Dans un arrêt protecteur des droits de l'homme tel que la CJUE les multiplie ces dernières années concernant Internet, la Cour a en effet jugé que les conditions n'étaient plus réunies pour être certain que les États-Unis respectent en droit et en fait la bonne protection des données personnelles des internautes européens traitées sur le sol américain. Elle a donc invalidé avec effet immédiat le Safe Habor qu'utilisaient des milliers d'entreprises américaines, dont Facebook, Google, ou Microsoft, ce qui aurait dû conduire à bloquer immédiatement tous les transferts de données vers les États-Unis, au moins le temps que les dossiers fondés sur d'autres mécanismes juridiques soient vérifiés et validés.

Or la CNIL et ses homologues ont décidé, sans aucune logique juridique mais par choix politique et pragmatique, d'octroyer aux États-Unis et à la Commission européenne un ultimatum fixé au 31 janvier 2016 pour négocier un nouveau Safe Harbor 2.0 assorti de nouvelles législations protectrices aux USA. « Quand nous avons appelé à une période de transition jusqu'en janvier, c'était un risque que nous avons pris ensemble. (…) Nous avons décidé de cette phase de transition afin de permettre à tous les acteurs du secteur de prendre leurs responsabilités », reconnaît aujourd'hui la présidente de la CNIL Isabelle Falque-Pierrotin, dans une interview à Euroactiv.

## « Les transferts de données ne continueront pas à n'importe quel prix »

Mais les négociations traînent, et les États-Unis n'ont toujours pas proposé de législation qui permettrait notamment aux Européens de faire valoir leurs droits contre la NSA, lorsque celle-ci accède à leur données sans contrôle judiciaire. En principe, le Safe Harbor 2.0 (s'il aboutit) ne devrait donc pas être plus sécurisant que l'ancien, et n'aura aucune validité pour légaliser les transferts des données.

## Interdire les transferts ? L'arme atomique

La menace de l'arme atomique de la suspension des transferts de données, brandie notamment en Allemagne, est donc théoriquement existante. Mais la CNIL peine à (se) convaincre d'une intention de l'utiliser, tant les enjeux économiques sont forts. « Nous souhaitons tous que les transferts de données continuent, parce qu'ils sont associés à des intérêts économiques et politiques très importants. Mais ils ne continueront pas à n'importe quel prix », prévient ainsi Mme Falque-Pierrotin.

Alors que le G29 avait demandé que des solutions juridiques soient trouvées avant la fin janvier 2016, le groupe se contente désormais d'exiger « un geste politique ».
« Je ne sais pas s'il sera possible de finaliser tout cela avant fin janvier, mais nous devons au moins recevoir un signe qu'ils ont compris le message des juges. Il ne s'agit pas de produire un Safe Harbor numéro deux. Il faut réellement tenir compte des arguments du juge, qui s'inquiète de la protection des données des citoyens européens aux États-Unis, quand les services de renseignement y ont accès », prévient la présidente du groupe des CNIL européennes.
Rendez-vous fin janvier pour voir quelles mesures seront effectivement prises.

---

Réagissez à cet article
Source : http://www.numerama.com/politique/134571-cnil-europeennes-safe-harbor-diplomatie-faiblesse.html