Décryptage du Safe Harbor | Le Net Expert Informatique

Décryptage du Safe Harbor

La Cour de justice de l'Union européenne (CJUE) a rendu la semaine dernière une décision historique en invalidant le « Safe Harbor ». Cet accord, concocté par le Département du Commerce des États-Unis, approuvé par la Commission européenne, légalise le transfert de données personnelles de citoyens européens vers les États-Unis. Amazon, Facebook et les autres géants américains du Net pouvaient donc librement exporter nos données et les exploiter à leur guise à des fins publicitaires. Son invalidation va changer la donne, et les défenseurs du respect de la vie privée, parmi lesquels l'UFC-Que Choisir, s'en réjouissent.

Le Safe Harbor en deux mots

Europe et États-Unis ont une vision différente de la protection des données personnelles des citoyens. Leurs politiques respectives en la matière sont donc divergentes. L'Europe interdit notamment le transfert des données personnelles vers des pays qui offrent un niveau de protection inférieur au sien (1). Pour ne pas priver les entreprises américaines de cet « or numérique » en provenance de l'Europe, le Département du Commerce des États-Unis (l'équivalent d'un ministère du Commerce) a concocté un cadre juridique qui légalise le transfert de données personnelles : le Safe Harbor, aussi appelé Sphère de sécurité. Les entreprises qui souhaitent en profiter doivent garantir certaines conditions (information des consommateurs sur l'exploitation de leurs données, droit de rectification, sécurité des données, etc.) et obtenir une certification. 4 000 entreprises américaines en sont titulaires, parmi lesquelles Microsoft, Amazon, Google ou encore Facebook.

De quelles données parle-t-on ?

Les données personnelles sont au centre de la plupart des modèles économiques des entreprises du Net. Vos achats, les messages que vous publiez sur les réseaux sociaux, vos habitudes de navigation sur Internet, les mots que vous saisissez dans les moteurs de recherche, ou bien encore les livres et les films que vous achetez en ligne sont autant d'indicateurs qui permettent de définir finement des profils de consommation et de vous envoyer des publicités ciblées, donc efficaces, donc vendues à prix d'or.

Quels sont les fondements de la décision de la CJUE ?

Tout est parti d'une plainte de Maximillian Schrems, un citoyen autrichien, auprès de l'autorité irlandaise de contrôle, l'Office of the Data Protection Commissioner, l'équivalent de notre Cnil (2). Maximillian Schrems utilise Facebook et sait qu'en vertu du Safe Harbor, ses données sont traitées aux États-Unis. Mais les révélations d'Edward Snowden, en 2013, sur la surveillance opérée par la NSA (National Security Agency) prouvent que le pays n'offre pas un niveau de protection suffisant des données. Or le Safe Harbor engage les États-Unis à fournir un niveau de protection au moins équivalent à celui de l'Europe.

La CJUE s'est prononcée sur deux points. D'abord, elle a confirmé qu'une autorité nationale (la Cnil et les autres) a le droit d'enquêter lorsqu'elle est saisie par un citoyen sur le sujet, et ce malgré l'existence du Safe Harbor. Ensuite, elle estime que la Commission européenne a eu tort d'accepter cet accord sans vérifier que les États-Unis n'interdisaient pas les opérations de surveillance généralisée (comme celles de la NSA). Du coup, 15 ans après son entrée en application, la justice suspend le Safe Harbor. Une décision historique.

Cette décision va-t-elle changer quelque chose ?

À court terme, les entreprises du Safe Harbor se retrouvent dans un trou juridique. Elles doivent subitement gérer une situation passée de légale à illégale du jour au lendemain. Les grandes entreprises disposent des armes suffisantes pour poursuivre leurs activités à coup de bras de fer juridiques. Mais quid des entreprises plus modestes ?

À moyen terme, l'Europe réaffirme son attachement à la protection des données personnelles. Cette décision de la CJUE pèsera sans doute dans les discussions sur le projet de Règlement européen sur les données personnelles. Ce texte, actuellement au stade des négociations tripartites entre le Parlement, le Conseil et la Commission, constituera à l'avenir le socle de la politique européenne en matière de protection de la vie privée.

(1) Directive 95/46/CE sur la protection des données personnelles.
(2) Commission nationale de l'informatique et des libertés.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.quechoisir.org/telecom-multimedia/internet/actualite-donnees-personnelles-decryptage-du-safe-harbor
Par Camille Gruhier

Que peuvent faire les entreprises en attendant un Safe Harbor II | Le Net Expert Informatique

Que peuvent faire les entreprises en attendant un Safe Harbor II

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Marc d'Haultfoeuille (Avocat Associé) et Nadège Martin (Avocat Of Counsel) de l'Equipe Technologie & Innovation de Norton Rose Fulbright, explique quoi faire en attendant un Safe harbor II.

Ce que les entreprises peuvent faire en attendant un Safe Harbor II

Force est d'admettre que la décision du 6 octobre 2015 par laquelle la Cour européenne de justice (CJUE) a déclaré invalide la décision Safe Harbor, sème un trouble auquel il n'existe aucune réponse juridique unanimement valable pour l'ensemble des entreprises concernées. Cette situation tient au fait qu'au-delà du contenu de cette décision, dont la portée demeure encore difficilement mesurable en l'absence de positionnement officiel des autorités de protection des données, d'autres paramètres doivent être pris en compte : le transfert est-il déjà effectif ? quelles sont ses finalités ? la loi nationale impose-t-elle des formalités préalables ?

AUDIT DES TRANSFERTS EN COURS

La décision de la CJUE étant d'application immédiate, depuis le 6 octobre 2015, tous transferts vers les Etats-Unis fondés sur le Safe Harbor sont invalides. Il est ainsi recommandé d'identifier rapidement les contrats et formalités déclaratives existants (ces transferts étaient soumis à simple notification auprès de la CNIL) afin de disposer des détails pertinents sur ces transferts.

Cet audit est nécessaire à l'identification des solutions alternatives envisageables à plus ou moins court terme, en l'état de la loi Informatique et Libertés ou sur la base des mesures qui pourraient être annoncées dans l'intervalle par la CNIL. A plus long terme, la décision Safe Harbor II en cours de discussion devrait être une solution pertinente mais il est difficile de prévoir sous quels délais elle sera adoptée.

DES DÉLAIS À ANTICIPER POUR LES TRANSFERTS À COURT TERME

La situation s'avère plus délicate pour les contrats en voie de conclusion pour lesquels le transfert était censé être fondé sur le Safe Harbor. En effet, sauf à pouvoir remplacer ce fondement par une exception légale ou des BCRs également soumis à simple notification préalable auprès la CNIL, les parties devront non seulement conclure des clauses contractuelles types (CCT) mais le responsable de traitement devra solliciter l'autorisation préalable de la CNIL au transfert. Or, obtenir cette autorisation peut prendre jusqu'à deux mois, voire plus, selon la loi. De plus, au vu des motifs de la décision rendue par la CJUE, le traitement de ces demandes par la CNIL est susceptible d'en être complexifié et en tout état de cause, allongé. Ces projets seront ainsi, pour beaucoup, dépendants des orientations qui seront prises par les autorités de protection des données.

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.usine-digitale.fr/article/ce-que-les-entreprises-peuvent-faire-en-attendant-un-safe-harbor-ii.N356084

Invalidation du « Safe Harbor » : quels sont les changements auxquels on doit s’attendre ? | Le Net Expert Informatique

La justice européenne a invalidé, mardi 6 octobre, l'accord « Safe Harbor » qui encadrait le transfert de données personnelles de l'Union européenne vers les Etats-Unis.

En quoi consiste Safe Harbor et que dit la Cour de justice de l'Union européenne (CJUE) ?
En Français « sphère de sécurité », le « Safe Harbor » est une décision de la Commission européenne, datant de 2000, qui affirme que le transfert de données personnelles d'Europe vers les Etats-Unis est possible car ce pays présente des garanties suffisantes pour la protection de la vie privée.
Très controversé, cet accord a notamment été mis à mal par les révélations d'Edward Snowden, en 2013, sur les programmes de surveillance de masse de la NSA. Les adversaires du Safe Harbor, dont Max Schrems, un Autrichien qui a déposé plusieurs plaintes contre Facebook, estimaient que ces révélations montraient que les données personnelles des Européens n'étaient en fait pas protégées lorsqu'elles étaient stockées aux Etats-Unis.
Dans son arrêt rendu mardi, la CJUE estime que le Safe Harbor n'est pas conforme au droit européen, pour plusieurs raisons détaillées sur une trentaine de pages. La Cour a notamment estimé que les recours possibles pour les citoyens européens estimant leurs droits malmenés étaient beaucoup trop faibles. Elle juge également que les programmes de surveillance de masse des Etats-Unis sont incompatibles avec une protection adéquate des droits des citoyens européens.

Cela veut-il dire que Facebook ne peut plus fonctionner en Europe, ou va devoir stocker les données des citoyens européens en Europe ?
Non : l'arrêt invalide un accord très générique. Facebook peut continuer à fonctionner comme il le faisait jusqu'à aujourd'hui, mais l'entreprise – tout comme Google ou tout autre entreprise qui stocke des données de citoyens européens aux Etats-Unis – ne peut plus s'abriter, en cas de procédure, derrière le fait qu'elle fait partie du Safe Harbor et que ses flux de données entre l'Europe et l'Amérique sont présumés légaux.
Facebook affirme en fait ne pas s'appuyer uniquement sur le Safe Harbor, mais « sur d'autres méthodes recommandées par l'Union européenne pour transférer légalement des données de l'Europe vers les Etats-Unis ».
Il existe en effet d'autres normes de transfert de données, comme par exemple les « clauses contractuelles type » ou les « règles internes d'entreprise » (dans le cas de transfert de données entre filiales), le Safe Harbor étant le cadre juridique simplifié et « par défaut ». Certaines entreprises du numérique utilisent déjà ces cadres juridiques alternatifs.
La Commission craint d'ailleurs que la décision de la CJUE ne favorise la multiplication de contrats spécifiques établis entre des entreprises et des pays européens, au détriment d'un cadre générique européen. Frans Timmermans, le vice-président de la Commission, a d'ailleurs annoncé que des « lignes directrices » à destination des autorités de protection des données seraient publiées afin d'éviter un « patchwork avec des décisions nationales ».
Par ailleurs, sans aller jusqu'à ces procédures juridiques, la loi européenne – plus spécifiquement l'article 26 de la directive de 1995 sur la protection des données personnelles – prévoit qu'un transfert vers un pays tiers peut être autorisé dans plusieurs cas. Par exemple, pour assurer la bonne exécution du contrat commercial (dans le cas d'une réservation d'hôtel par exemple, où les coordonnées du client sont nécessaires) ou lorsque intervient le consentement explicite de l'internaute à ce que ses données soient transférées.

Le Safe Harbor va-t-il être renégocié ?
La renégociation de cet accord était déjà en cours avant l'arrêt de la Cour. Malgré l'expiration de plusieurs dates butoirs, les négociateurs ont récemment affirmé qu'ils faisaient des progrès dans les discussions. Mais il sera difficile d'obtenir rapidement un accord qui puisse satisfaire les exigences de la CJUE : cette dernière rappelle dans son arrêt que, pour obtenir un régime de ce type, un pays doit faire la preuve qu'il offre des garanties de protection de la vie privée comparables à celles en vigueur au sein de l'UE.
Cela signifie qu'il faudrait des changements majeurs dans le droit américain pour qu'un nouvel accord ne soit pas, à son tour, invalidé par la Cour.

Que se passe-t-il dans l'immédiat ?
Plus de 4 000 entreprises étaient soumises à l'accord Safe Harbor. Nombre d'entre elles, particulièrement les plus petites, se retrouvent brusquement, au moins jusqu'à l'adoption d'un nouvel accord Safe Harbor, dans un vide juridique.
Les grands acteurs du Web, eux, sont dans l'attente. L'annulation du Safe Harbor semble les avoir pris de court. Dans un communiqué, l'association professionnelle Digital Europe, qui regroupe tous les grands acteurs du secteur (d'Apple à Toshiba en passant par Google, à l'exception de Facebook), « demande de toute urgence à la Commission européenne et au gouvernement américain de conclure leurs négociations pour parvenir à un nouvel accord "Safe Harbor" aussi vite que possible ».
« Nous demandons également à la Commission européenne d'expliquer immédiatement aux entreprises qui fonctionnaient sous le régime du Safe Harbor comment elles doivent opérer pour maintenir leurs activités essentielles durant ce vide juridique », poursuit l'association.
Facebook a, de son côté, estimé également qu'il « fallait impérativement que les gouvernements européens et américain donnent des méthodes légales pour le transfert des données et règlent toutes les questions de sécurité nationale ».

Quelles seront les conséquences plus larges de cette décision ?
Si l'arrêt de la CJUE ne porte que sur le Safe Harbor, il dénonce avec des mots très durs les programmes de surveillance de masse de la NSA américaine, présentés comme incompatibles avec les droits fondamentaux garantis par le droit européen.
Le jugement pourrait aussi influencer deux dossiers européens brûlants dont les négociations arrivent dans leur dernière ligne droite : l'accord « parapluie » sur l'échange de données personnelles pour la coopération policière, entre Europe et Etats-Unis, et le projet de règlement sur les données personnelles.
La commissaire européenne à la justice, Vera Jourova, a indiqué que l'arrêt de la Cour confortait la position de la Commission, notamment sur la nécessité d'avoir « des garde-fous solides » en matière de protection des données.
Washington s'est dit « déçu » par la décision de la justice européenne, estimant qu'elle créait une « incertitude pour les entreprises et les consommateurs à la fois américains et européens et met en péril l'économie numérique transatlantique qui est en plein essor ».

Source : http://www.lemonde.fr/pixels/article/2015/10/06/safe-harbor-que-change-l-arret-de-la-justice-europeenne-sur-les-donnees-personnelles_4783686_4408996.html

La CNIL entend imposer un droit à l’oubli bien au delà des frontières européennes | Le Net Expert Informatique

	La CNIL entend imposer un droit à l’oubli bien au delà des frontières européennes

La CNIL entend imposer un droit à l'oubli très large, bien au delà des frontières européennes. Va-t-elle avoir gain de cause?

La CNIL contre Google. David contre Goliath. A elle seule, l'affiche du duel suscite l'admiration. Il en faut du courage, une noble cause et des convictions bien trempées, pour croiser le fer avec un acteur mondial si puissant.
Le 21 septembre, Madame Isabelle Falque-Pierrotin, Présidente de la CNIL, a confirmé sa décision d'imposer à Google d'effacer, dans le monde entier, les résultats de recherche portant sur le nom d'une personne, lorsque ces résultats ne sont pas jugés nécessaires à l'information du public en France.
D'après le communiqué de la CNIL, cette décision serait la simple conséquence d'un arrêt rendu le 13 mai 2014 par la Cour de Justice de l'Union Européenne (CJUE). La CNIL se bornerait à « demander le plein respect du droit européen par des acteurs non européens offrant leurs services en Europe ». En outre, cette décision ne porterait pas atteinte au droit à l'information du public situé hors d'Europe, puisque les contenus déréférencés sur les moteurs de recherche resteraient toujours accessibles, à condition de les trouver autrement qu'en recherchant le nom d'une personne. Enfin, cette décision serait très strictement encadrée, puisque « placée sous le double contrôle de la CNIL et du juge »… français.

Google entend se conformer strictement à la législation locale
Google, pour sa part, estime devoir se conformer à la législation locale -française et européenne- en respectant les frontières juridiques et territoriales de la loi locale. Le géant américain admettrait de supprimer les résultats de recherche accessibles sur ses services destinés aux internautes européens (« .fr », « .de », « .co.uk », etc), mais pas pour ceux du monde entier.
Tous les arguments de la CNIL sont simples : quand elle demande la désindexation d'une information rapportée par un moteur de recherche et dont se plaint un ressortissant européen, c'est pour le monde entier. Peu importe l'organe de presse ou la liberté d'expression garantie dans le pays diffusant l'information en cause. Peu importe l'endroit du monde depuis lequel un internaute consulterait un moteur de recherche.
On voudrait y croire. Oublier les frontières, exporter nos valeurs, comme au Siècle des Lumières… Mais le faire en 2015, sur Internet, sans un instrument juridique international négocié entre Etats, c'est soit prétentieux, soit voué à l'inefficacité. Ou probablement les deux.

La simplicité ne suffit pas à faire la loi
Le droit européen et français s'impose principalement aux entreprises européennes, ainsi qu'aux entreprises non-européennes qui traitent ou font traiter des données personnelles sur le sol européen. Mais le fait d'offrir des services en Europe n'est pas, à l'heure actuelle, un critère suffisant pour appliquer à un acteur extra-européen nos règles européennes de protection de la vie privée.

On peut en être frustré, mais c'est l'état du droit en vigueur. Cette situation changera probablement dans deux ans, après que l'Union européenne aura adopté un projet de Règlement sur la protection des données personnelles. Ce projet est encore en cours de rédaction et on espère le voir finalisé dans quelques semaines -la fin de l'année 2015.

La CNIL anticipe donc des critères d'application du droit français et européen qui n'existent pas encore. En droit, il s'agit de déterminer si notre loi française « Informatique & Libertés » est une loi dite « de police ». Il s'agit de justifier qu'elle ait des effets contraignants hors de notre territoire national à l'encontre d'un acteur qui ne fabrique pas son moteur de recherches sur le sol européen.

Divergences de jurisprudence
La jurisprudence judiciaire française est divergente sur ce point. Déjà en juin 2011, l'Assemblée nationale, dans son rapport sur les « Droits de l'individu dans la révolution numérique », constatait que « la protection des données personnelles […] n'obéit aujourd'hui à aucun caractère juridique universel et contraignant », soulignant alors la nécessité de réformer le cadre européen adopté en 1995 . Et l'Assemblée de conclure qu' « il appartient aux pouvoirs publics des États concernés et non aux autorités de contrôle de réfléchir à la nécessité de mettre en œuvre l'adoption d'une convention internationale ».

Le Conseil d'État, pour sa part, dans son rapport d'études pour l'année 2014 , a listé les conditions à réunir : si le futur règlement européen sur la protection des données s'étend aux entreprises établies hors de l'Union européenne au motif qu'elles offrent leurs services en Europe et si les droits en cause sont garantis par la Charte des Droits Fondamentaux de l'Union européenne , on pourra alors qualifier de « lois de police » les règles de protection des données personnelles adoptées par l'Union européenne. Or, ces deux conditions ne sont pas réunies aujourd'hui.

Les autorités européennes elles-mêmes -la CNIL et ses homologues-, ont appelé en novembre 2014, dans une déclaration solennelle , à ce que ces futures règles européennes soient dites « d'ordre public international » – ou « de police » -, car elles devraient avoir des effets partout dans le monde. Mais ces déclarations, qui n'ont aucun caractère normatif, montrent précisément que ce qui « devrait être », n'est pas encore.

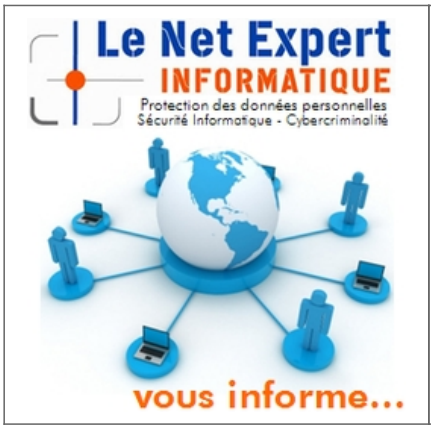
Sanctionner avant d'avoir régulé ?
Si Google résiste aux injonctions de la Présidente de la CNIL, cette dernière réunira dans les prochains jours la formation restreinte de la CNIL, qui est seule habilitée à prononcer un avertissement, une amende administrative plafonnée à 150 000 -ou 300 000 euros en cas de récidive-, voire une injonction de cesser le traitement illicite de données. Si la CNIL condamne et si son raisonnement est contesté par Google, ce débat pourra faire l'objet d'un recours devant le Conseil d'Etat, puis rebondir devant la CJUE, conduisant celle-ci à statuer dans quelques années.

Toutefois, la pression juridique exercée sur un acteur privé, fut-il un Léviathan, ne peut pas se substituer à l'absence de règles de droit international ou de traités bilatéraux. Ce débat ne peut donc se limiter longtemps à un rapport de forces entre un régulateur national ou européen et un acteur économique mondial. Car ce rapport de forces serait perdu d'avance par un régulateur impatient. Tout le paradoxe est là : la CNIL pourra prononcer des sanctions, même fortes, cela ne haussera pas le niveau de protection des données personnelles hors de l'Union européenne, tant qu'un accord international entre Etats ne sera pas trouvé.

En initiant un combat homérique deux ans avant d'être confortée par un texte ou contredite par un juge, la Présidente de la CNIL se garantit un feuilleton médiatique à rebondissements. Pour quelle efficacité réglementaire ? A chacun ses objectifs et son agenda.

Source : http://www.latribune.fr/opinions/tribunes/droit-a-l-oubli-la-cnil-a-la-conquete-du-monde-509984.html
Par Etienne Drouard, avocat au Barreau de Paris

La gestion des comptes personnels de formationencadrés par la CNIL (Commission nationale de l’informatique et des libertés) | Le Net Expert Informatique



La gestion des comptes personnels de formationencadrés par la CNIL (Commission nationale de l’informatique et des libertés)

Découvrez les règles relatives à la gestion des comptes personnels de formation avec la CNIL (Commission nationale de l'informatique et des libertés).
Autorisation Unique n° AU-044 – Délibération n° 2015-227 du 9 juillet 2015 portant autorisation unique de traitements de données à caractère personnel mis en œuvre aux fins de gestion des comptes personnels de formation (AU-44)

Consultez la délibération

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.cnil.fr/documentation/deliberations/deliberation/delib/336/

Qui protège le mieux ses données personnelles ? | Le Net Expert Informatique

Qui protège le mieux ses données personnelles ?

La récente affaire Ashley Madison a démontré une nouvelle fois les nombreuses failles de nos systèmes informatiques et la négligence des utilisateurs à confier leurs données personnelles à tous types de sites. Newmanity au travers de son étude a voulu étudier le comportement des français face à cette polémique et les résultats s'avèrent des plus surprenants ! Homme, femme, qui a le plus peur pour ses données personnelles ?

L'échantillon
Enquête réalisée auprès d'un échantillon de Français recrutés par téléphone puis interrogés par Internet les 31 août et 1er septembre 2015. Echantillon de 1183 personnes, représentatif de la population française âgée de 18 ans et plus. La représentativité de l'échantillon est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, profession du chef de famille et profession de l'interviewé après stratification par région et catégorie d'agglomération.

Ce qu'il faut retenir de l'étude
La majorité des actifs Français déclarent faire plus attention à leurs données numériques dans le cadre personnel, plutôt que dans le cadre professionnel > Les hommes déclarent protéger davantage leurs données que les femmes.
Les Français expriment plus de méfiance à l'égard des appareils mobiles (Smartphones, Tablettes) que des ordinateurs > La déconnexion des comptes est une habitude peu fréquente pour les Français

Les hommes plus méfiants que les femmes
Selon les actifs français, les données numériques les plus préoccupantes sont celles issues d'une utilisation personnelle : 69% d'entre eux déclarent y être plus vigilants contre 28% dans le cadre professionnel. Et ce sont les femmes qui sont les moins regardantes (34%) sur la protection de leurs données dans le cadre personnelles contre 73% des hommes qui scrutent méticuleusement la moindre trace sur la toile !
Paradoxalement, les manipulations de base permettant de limiter les problèmes de sécurité en matière de données numériques sont encore assez peu utilisées :
Se déconnecter d'une boîte mail : Moins de 6 actifs sur 10 se déconnectent systématiquement de leur boite mail personnelle lorsqu'ils la consultent depuis le bureau, et cette proportion tombe à 48% lorsque l'utilisation se fait sur ordinateur personnel.
Suppression de l'historique de navigation : Que ce soit sur leur ordinateur personnel ou professionnel, moins de 4 Français sur 10 suppriment leurs données de navigation tous les jours ou au moins une fois par semaine. D'ailleurs, près de 3 actifs sur 10 ne suppriment jamais leur historique de navigation sur leur ordinateur professionnel. Des gestes pourtant simples qui permettraient une meilleures protection de la vie privée de tout un chacun.

Les appareils mobiles suscitent plus de méfiance
Près de la moitié des Français détenteurs d'équipements numériques n'en n'ont pas confiance, signe d'une certaine méfiance alors que les affaires de piratage de données personnelles (Orange, Ashley Madison…) font régulièrement la Une de l'actualité. Dans le détail, que ce soit à l'égard des ordinateurs personnels ou professionnels, les cadres et les femmes qui semblent être les plus confiants. A l'inverse, les hommes et les CSP 'employés' et 'ouvriers' sont nettement plus réservés.
Il est à noter que cette méfiance devient défiance lorsqu'il s'agit de tablettes ou de smartphones. Ces équipements mobiles sont marqués par le peu de confiance qui leur est accordé en matière de sécurité de données transmises : Seulement 37% des Français détenteurs d'une tablette numérique lui font confiance et à peine plus d'un tiers (34%), en ce qui concerne les possesseurs de smartphones.

Source : http://www.economiematin.fr/news-internet-securite-utilisateurs-protection-donnees
Par Stéphane Petibon

Les Cnil européennes peuvent-elles condamner un éditeur de site étranger ? | Le Net Expert Informatique

	Les Cnil européennes peuvent-elles condamner un éditeur de site étranger ?

Le responsable du traitement de données personnelles d'un pays de l'UE peut se voir appliquer le droit d'un autre Etat membre. La Cour de Justice de l'Union européenne vient de statuer dans une affaire opposant un site slovaque à la Cnil hongroise, considérant que les régulateurs sont compétents pour condamner un éditeur de site étranger si celui-ci exerce sur le sol national.

Un site Web, même immatriculé à l'étranger (en l'occurrence dans un autre État membre de l'UE), peut se voir appliquer le droit d'un État membre relatif à la protection des données personnelles, pour peu que l'éditeur de ce site exerce « au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué ». C'est en substance l'arrêt qu'a publié hier la CJUE.

L'affaire opposait un site d'annonces immobilières slovaque et la Cnil hongroise. La société slovaque, refusant de supprimer gratuitement les données personnelles de clients hongrois, avait été condamnée à une amende par la Nemzeti Adatvédelmi és Információszabadság Hatóság (l'équivalent hongrois de notre Cnil). L'éditeur du site a par la suite contesté la compétence territoriale de la NAIH : l'affaire termina devant la Cour suprême de Hongrie, qui a soumis la question à la CJUE.

Compétence territoriale précisée

Laquelle vient de rendre un arrêt on ne peut plus clair sur la compétence territoriale des Cnils européennes. Elle considère que le droit européen « permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé ». Indépendamment de la nationalité des victimes, à la seule condition que « le responsable du traitement des données » exerce une activité dans l'État membre concerné.

En outre, précisent les juges, si l'autorité de contrôle d'un État membre estime que ce n'est pas le droit national qui doit s'appliquer, mais celui d'un autre État membre, « elle ne saurait infliger de sanctions sur la base du droit de cet État membre au responsable du traitement de ces données qui n'est pas établi sur ce territoire ». Toutefois, elle peut saisir la Cnil du second État membre. Il revient dès lors à la juridiction nationale de déterminer si la société « étrangère » exerce sur son sol, « au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime ».

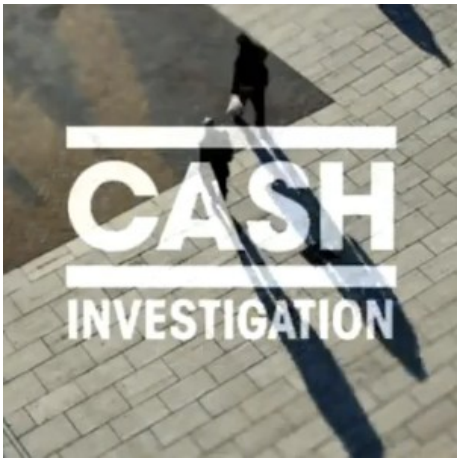
Evidemment, cet arrêt ne concerne que les éditeurs responsables du traitement de données à caractère personnel établis sur le territoire de l'UE. Mais, considérant qu'un certain nombre de géants du Web disposent de sièges en Europe, la jurisprudence pourrait bien être utilisée contre eux, ce qui suscitera sans aucun doute de nouveaux débats juridiques et, qui sait, une nouvelle jurisprudence.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.linformaticien.com/actualites/id/38047/les-cnil-europeennes-peuvent-elles-condamner-un-editeur-de-site-etranger.aspx
par Guillaume Périssat

Données personnelles : mais à quoi sert la CNIL ? – Cash

Investigation ce mardi 6 octobre 2015 | Le Net Expert Informatique



Données personnelles : mais à quoi sert la CNIL ? – mardi 6 octobre 2015

Certaines associations caritatives vendent en toute illégalité leurs fichiers de donateurs à La Poste. Face à Elise Lucet, la présidente de la CNIL ne semble pas au courant et se déclare « surprise ». Un extrait de « Cash Investigation » diffusé sur France 2 le mardi 6 octobre à 20h55. Lire la suite….

Ci-dessous, le rapport d'activité 2014 de la CNIL dont il est fait mention dans le reportage (Merci à Eric EGÉA) :

http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-35e_rapport_annuel_2014.pdf.pdf

---

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

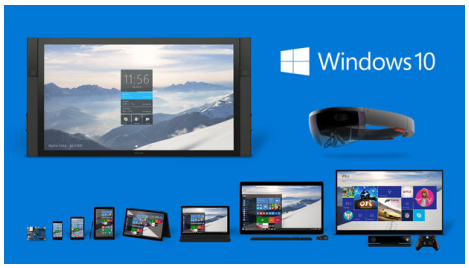
Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

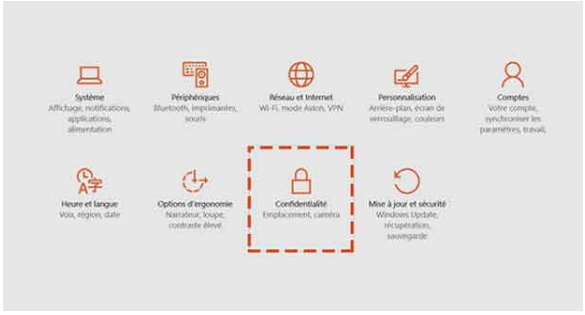
http://www.francetvinfo.fr/internet/cash-investigation-donnees-personnelles-mais-a-quoi-sert-la-cnil_1109973.html

Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique | Le Net Expert Informatique

	Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique

Windows 10 est disponible gratuitement pour les PC sous Windows 7 ou Windows 8.1. Il propose des changements face à ses prédécesseurs dont certains touchent à la surveillance, l'analyse et la collecte de données personnelles concernant ses utilisateurs. La CNIL met en garde et propose un tutoriel pour se protéger des yeux indiscrets de la firme.

En France, la CNIL a rapidement réagi devant les nombreux systèmes de surveillance et de collecte de données accompagnant Windows 10. Dans un dossier mis en ligne quelques jours seulement après le lancement de l'OS, elle propose « quelques réglages de confidentialité qui permettent de limiter la communication de vos informations à l'éditeur et à ses partenaires ».



Windows 10, des fuites dans Cortana, Microsoft Edge ou encore la synchronisation

Ils se concentrent sur trois thèmes, Cortana avec un paramétrage de la » vie privée « , la synchronisation des comptes sur les autres appareils utilisés et le navigateur Microsoft Edge.

Elle recommande ainsi de désactiver la géo-localisation, d'empêcher la collectes de données liées à l'Appareil photo, le Microphone, les Informations de Compte, des Contacts, du Calendrier, de la Messagerie, des communications Radio ou encore d'agir sur la fonctionnalité » apprendre à me connaître » pour la dictée vocale. Au sujet du nouveau navigateur, Microsoft Edge, il est recommandé de désactiver l'option » Utiliser la prédiction de page pour accélérer la navigation, et améliorer le mode lecture ainsi que mon expérience globale » puisque celle-ci requiert d'envoyer votre historique de navigation tandis l'obtention de suggestions de recherche demande qu'une grande partie des informations que vous saisissez dans la barre de navigation soit envoyée au moteur de recherche Bing. Il est donc recommandé de désactiver « Afficher les suggestions de recherche à mesure que je tape « .

Vous trouverez ici, un pas à pas complet pour reprendre la main sur vos données personnelles : Régler les paramètres vie privée de Windows 10

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.ginjfo.com/actualites/logiciels/windows-10/windows-10-et-sa-vie-privee-la-cnil-met-en-garde-et-une-fiche-pratique-20150928

Safe Harbor remis en question – Et si le transfert de

données personnelles aux US cessait ? | Le Net Expert Informatique

Safe Harbor remis en question – Et si le trans

Pour l'avocat général de la CUJE, la disposition autorisant les transferts de données vers les Etats-Unis (Safe Harbor) est invalide car le pays ne garantit pas la protection de ces données du fait de la surveillance par la NSA. Une Cnil européenne a de plus tout pouvoir pour suspendre ces transferts.

Entre Maximilian Schrems et Facebook, c'est une longue histoire d'amour (vache). C'est notamment à ce dernier qu'on doit d'avoir découvert l'ampleur de la collecte de données personnelles effectuée par le réseau social.
Remonté contre les pratiques de Facebook, le jeune autrichien l'est tout autant à l'encontre de la surveillance massive par les Etats-Unis. Pour accéder aux données des Européens, la NSA pourrait compter sur un dispositif : le Safe Harbor.

Une « des voies » des agences US pour accéder « à la collecte des données »

Le Safe Harbor prévoit le transfert automatique de données par les entreprises entre l'Europe et les Etats-Unis. C'est cet accord qui est visé par Maximilian Schrems au travers de sa plainte contre Facebook devant la justice irlandaise.
Le justiciable européen conteste le transfert de données à caractère personnel de Facebook Ireland à Facebook USA au motif que la protection de ses données n'est pas garantie du fait du programme PRISM de la NSA.
Saisie par la Haute Cour de Justice d'Irlande, la Cour de Justice européenne est appelée à se prononcer sur plusieurs points de droit. Pour l'heure, c'est l'avocat général de la CUJE, Yves Bot, qui a livré son analyse juridique.

Et en substance, ce dernier souligne le manque de garanties entourant le Safe Harbor et estime qu'une autorité nationale de protection peut enquêter sur les transferts de données réalisées dans ce cadre.

Plus encore, écrit l'avocat général, une autorité, au terme de ses investigations, « a le pouvoir de suspendre le transfert de données en cause » dès lors qu'elle estime qu'il « porte atteinte à la protection dont doivent bénéficier » les citoyens de l'UE.
Le Safe Harbor part du postulat que les Etats-Unis apportent un niveau de protection adéquat. Une obligation cependant qui se doit d'être continue, souligne Yves Bot. Cela « suppose qu'aucune circonstance intervenue depuis ne soit de nature à remettre en cause l'évaluation initiale effectuée par la Commission. »
Or, les révélations d'Edward Snowden au sujet de la surveillance par la NSA pourraient justement constituer une remise en cause. La Commission de l'UE elle-même estimait que le Safe Harbor était « l'une des voies par lesquelles les autorités américaines de renseignement ont accès à la collecte des données à caractère personnel initialement traitées au sein de l'Union. »

La « décision 2000/520 doit être déclarée invalide »

Pour l'avocat général de la CUJE, le « droit et la pratique des États-Unis permettent de collecter, à large échelle, les données à caractère personnel de citoyens de l'Union qui sont transférées dans le cadre du régime de la sphère de sécurité, sans que ces derniers bénéficient d'une protection juridictionnelle effective. »
C'est donc le principe même du Safe Harbor et des transferts automatisés de données qui est contesté. « Nous sommes, dès lors, d'avis que la décision 2000/520 doit être déclarée invalide dans la mesure où l'existence d'une dérogation qui permet d'une manière aussi générale et imprécise d'écarter les principes du régime de la sphère de sécurité empêche par elle-même de considérer que ce régime assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées aux États-Unis depuis l'Union » va jusqu'à considérer le représentant de la CUJE.
« C'est formidable de voir que l'avocat général a utilisé cette affaire pour rendre un avis général sur les transferts de données vers des pays tiers et la surveillance de masse » réagit Maximilian Schrems.
« Si le système du Safe Harbor disparaît, il est très probable que les autorités de protection dans les 28 Etats membres de l'UE n'autoriseront pas les transferts de données des entreprises US soumises à des lois de surveillance de masse » ajoute-t-il.
Les géants américains du Web comme Facebook pourraient ainsi se voir interdire le droit de transférer les données des utilisateurs européens de leurs services vers les Etats-Unis. Les juges de la Cour de Justice de l'UE doivent toutefois rendre leur décision, en tenant compte ou non de l'avis de l'avocat général.

Source : http://www.zdnet.fr/actualites/safe-harbor-et-si-le-transfert-de-donnees-personnelles-aux-us-cessait-39825358.htm
Par Christophe Auffray