

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 Harbor 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>

Directive sur la cybersécurité : Amazon, eBay, Google devront notifier leurs incidents majeurs – Next INpact



Après des heures de négociations, le Parlement européen et les États membres sont arrivés lundi à un accord sur la future directive NIS (network and information security). Un texte destiné à mieux protéger les opérateurs dits critiques dans toute l'Europe.



Cette future directive sur la cybersécurité visera en effet à imposer des règles harmonisées à tout un ensemble d'opérateurs critiques. Le mouvement sera épaulé par le réseau des Computer Security Incident Response Team (CSIRT) pour discuter des incidents et identifier de possibles réponses coordonnées.

Plusieurs niveaux de reporting selon les acteurs concernés

Ce texte visera avant tout à définir des critères pour savoir qui relève de ces obligations. En tête de liste, on trouvera nécessairement les acteurs de l'énergie, du transport et de la santé. Selon l'eurodéputé Andreas Schwab (EPP), ces entreprises devront répondre à plusieurs mesures de sécurité, mais également notifier aux autorités les incidents de cybersécurité qualifiés « d'importants. »

Si les micro entreprises et les PME seront épargnées, les principaux acteurs du Net seront également concernés, mais avec des obligations finalement plus en retrait. Sont cités les marketplaces comme Amazon ou eBay, les moteurs de recherche mais aussi les services de cloud qui devront mettre en place de mesures de sécurité tout en rapportant aux autorités les seuls « incidents majeurs » qui viendraient les impacter.

Le flou règne par contre sur les autres plateformes en ligne comme les réseaux sociaux. Selon l'eurodéputé, toutefois, « cette directive marque le début de la régulation des plateformes. Alors que la consultation de la Commission européenne sur ces acteurs est toujours en cours, les nouvelles règles prévoient déjà des définitions concrètes – une demande du Parlement européen exprimée depuis le début des négociations –, afin de faire connaître son consentement à l'inclusion des services numériques. »

En août dernier, l'obligation de reporter aux autorités les incidents de sécurité avait soulevé les inquiétudes des représentants du secteur. Selon l'Afdel, l'association française des éditeurs de logiciels et de solutions Internet, une obligation indifférenciée de reporting « pourrait porter atteinte à la compétitivité des entreprises du numérique, en particulier des entreprises françaises et européennes du numérique – dont de nombreuses PME, qui n'ont pas toute la capacité d'adaptation des grands groupes internationaux –, sans atteindre les objectifs poursuivis en termes de sécurité ». L'ASIC, l'association des services Internet communautaires, avait craint pour sa part de voir chaque État membre devenir « le Directeur des services informatiques de l'ensemble des acteurs du numérique », du moins si des critères trop larges étaient inscrits en dur dans le texte final.

Le projet de directive doit maintenant être approuvé formellement par la Commission au marché intérieur du Parlement européen et par le Comité des représentants permanents.

Des obligations de reporting préexistent dans certains secteurs et en France

Suite à l'adoption du Paquet Télécom en Europe, rappelons que les opérateurs télécom doivent déjà notifier les fuites de données personnelles aux autorités de contrôle des données personnelles (la CNIL, [ici](#)). En France, l'Agence nationale de la sécurité des systèmes d'information chapeaute pour le compte du premier ministre, les règles de sécurité que doivent suivre les OIV, ces opérateurs d'importance vitale dont l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.

Depuis la loi de programmation militaire de 2013, centrales nucléaires, hôpitaux, sociétés de transports, acteurs des télécoms, etc. ont l'obligation de fournir « les informations nécessaires pour évaluer la sécurité de ses systèmes d'information, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que les codes sources de ces logiciels. »



Réagissez à cet article

Source

<http://www.nextinpact.com/news/97630-directive-sur-cybersecurite-amazon-ebay-google-devront-notifier-leurs-incidents-majeurs.htm>

La CNIL demande à Facebook de ne pas tracer les non-membres



À la suite du jugement belge exigeant de Facebook qu'il mette fin au pistage des internautes, cinq autorités de protection de la vie privée demandent au réseau social d'appliquer les conséquences du verdict sur l'ensemble de l'Union européenne.

Dans son bras de fer contre Facebook, qui est accusé de suivre tous les internautes à la trace, y compris ceux qui ne sont pas inscrits sur le réseau social, la commission de la protection de la vie privée belge n'est pas seule. L'institution peut en effet compter sur le soutien de quatre autres autorités européennes.

Celles-ci ont en effet publié une déclaration commune qui réclame la fin de l'ingérence du site américain dans la vie privée des internautes. Ce texte fait suite au jugement rendu en première instance par le tribunal civil de Bruxelles, qui condamne Facebook à cesser de tracer l'activité des internautes en Belgique lorsqu'ils visitent des sites web sur lesquels sont installés des boutons de partage, comme le célèbre « J'aime ».

Les autorités de France, de Belgique, d'Espagne, des Pays-Bas et de Hambourg sur la même ligne.

« Tout en reconnaissant le droit de Facebook à faire appel de ce jugement, le Groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne », écrivent-elles. Elles ajoutent, dans un communiqué, que cette immixtion « n'est pas acceptable » et que Facebook doit « prendre les mesures nécessaires pour se mettre en conformité » avec les règles communautaires.

Mais en la matière, les mesures que Facebook a déjà déployées pour respecter le jugement de la justice belge ont eu pour effet d'irriter la commission de la protection de la vie privée belge. En effet, au lieu de neutraliser le cookie litigieux (intitulé « datr » et que Facebook justifie au nom de la sécurité de ses membres), le réseau social a préféré bloquer l'accès aux internautes belges qui ne sont pas connectés au service.



Réagissez à cet article

Source

<http://www.numerama.com/politique/133980-la-cnil-demande-a-facebook-de-ne-pas-tracer-les-non-membres.html>

Safe Harbor et localisation des données

 <p>Denis JACOPINI</p> <p>vous informe LCI</p>	<p>Safe Harbor et localisation des données</p>
---	--

Après l'invalidation du Safe Harbor, Max Schrems pousse son avantage, et veut obliger les CNIL européennes à tirer les conséquences de la fin de cet accord. Et à obliger les GAFAs à stocker les données personnelles des Européens sur le continent.



Un jeune Autrichien en 28 ans va-t-il faire plus pour la régulation du Cloud sur le Vieux Continent que la Commission Européenne depuis dix ans ? L'activiste Maximilian Schrems, (en photo) déjà à l'origine de l'invalidation de l'accord dit Safe Harbor par la Cour de justice européenne (CJUE), ouvre un nouveau front, touchant cette fois à la localisation des données personnelles des citoyens européens.

Sa cible, une fois encore : Facebook.

Schrems demande cette fois à plusieurs CNIL en Europe d'ordonner au réseau social de conserver ses données sur le sol européen, arguant du fait qu'il n'existe plus (et pour cause) de cadre légal assurant le transfert de ses données sur le sol américain en toute sécurité. Pour ce faire, l'activiste a déposé deux nouvelles plaintes contre Facebook. La première auprès de l'autorité belge de protection des données, la seconde auprès de l'équivalent de la CNIL en Allemagne. Max Schrems a également mis à jour sa plainte auprès de l'autorité irlandaise, celle qui avait abouti à l'invalidation du Safe Harbor. Rappelons que Facebook opère ses activités hors des Etats-Unis depuis l'Irlande, raison pour laquelle Schrems avait choisi ce pays pour s'attaquer au réseau social. L'autorité irlandaise s'étant déclaré incompétente, la plainte avait été transmise à la CJUE qui avait fini par invalider le Safe Harbor, accord de 2001 autorisant les entreprises établies aux Etats-Unis, notamment les GAFAs (Google, Apple, Facebook, Amazon), à recevoir des données en provenance de l'Union européenne dans un cadre légal. La CJUE a décidé de tirer un trait sur cet accord à la lumière des révélations d'Edward Snowden sur les programmes de surveillance de la NSA et sur la complicité des grands noms du Web – dont Facebook – à ces programmes.

Forcer la main des CNIL européennes

Cet accord n'existant plus, Max Schrems estime que les transferts de données vers les Etats-Unis violent la loi européenne, qui réclame que ces exports ne peuvent être effectués vers un pays offrant un niveau de protection inférieur à celui de la loi en place sur le Vieux Continent. Le jeune Autrichien se demande donc sur quelles bases légales sont assurés les transferts de ces données vers les Etats-Unis. Interpelé sur ce point le 12 octobre (quelques jours après la décision de la CJUE), Facebook a produit tardivement un accord contractuel, daté du 20 novembre 2015, passé entre sa filiale irlandaise et sa maison mère et encadrant les transferts d'informations entre les deux entités. « En plus de cet accord, Facebook Ireland se base sur un certain nombre d'autres moyens légaux pour transférer les données de ses utilisateurs aux Etats-Unis », assurent les avocats du réseau social, dans une lettre. Sans plus de précisions toutefois. Max Schrems conteste la légalité de ces accords, censés suppléer la disparition du Safe Harbor, au regard des révélations d'Edward Snowden sur des programmes de surveillance comme Prism.

Pour forcer les CNIL européennes à prendre ce qu'il estime être tirer les conséquences logiques de la décision de la CJUE, le jeune Autrichien pourra s'appuyer sur les fractures qui apparaissent entre ces différentes autorités de contrôle. Fin octobre, l'administration allemande a mis en doute la voie préconisée par la Commission européenne après la fin du Safe Harbor, soit la mise en place rapide d'alternatives basées sur des accords contractuels. Indiquant qu'elle bloquerait tout nouveau transfert de données exploitant ces mécanismes.

Conséquence, selon Johannes Caspar, le responsable allemand de la protection des données : « Quiconque souhaite échapper aux conséquences légales et politiques du jugement de la CJUE devrait dans le futur étudier le stockage des données personnelles uniquement sur des serveurs situés au sein de l'UE ».

Max Schrems explique que les plaintes déposés en Irlande, en Belgique et en Allemagne font partie d'un « premier round » ; d'autres devraient suivre dans d'autres juridictions européennes.

Dans un communiqué, l'activiste précise : « je n'ai aucune doute qu'une large majorité des autorités européennes de protection des données enquêteront correctement sur les plaintes et prendront les actions qui s'imposent. Néanmoins, dans un cas particulier, j'ai senti le besoin de clarifier le fait qu'une résistance délibérée à faire le travail pourrait avoir des conséquences personnelles pour les responsables concernés ».

Safe Harbor 2 dans l'urgence

Rappelons que, suite à l'invalidation du Safe Harbor, la Commission européenne a relancé dans l'urgence des négociations pour aboutir rapidement à un nouvel accord cadre. Ce Safe Harbor 2 devra répondre pleinement aux exigences de la CJUE, pour que le cadre résiste aux défis juridiques posés par les régulateurs en charge de la protection des données.

Réunis au sein du groupe des CNIL européennes (G29), ces derniers attendent des autorités européennes et américaines une solution « satisfaisante » avant le 31 janvier 2016. Nul doute que Max Schrems n'est de toute façon pas disposé à leur laisser davantage de temps.



Réagissez à cet article

Source : <http://www.silicon.fr/max-schrems-le-tombeur-du-safe-harbor-sattaque-a-la-localisation-des-donnees-133129.html>

Des amendes plus lourdes de la part de la Cnil ? – Denis JACOPINI Expert informatique

Denis JACOPINI



vous informe

Des amendes plus
lourdes de la
part de la Cnil
?