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*

Loi sur le numérique adoptée quasiment sans voix contre

#Loi sur le numérique adoptée quasiment sans voix contre

La loi Pour une république numérique » vient d'être adoptée par l'Assemblée Nationale à 356 contre 1. Elle sera prochainement examinée au Sénat pour une seconde lecture.
La loi sur le numérique d'Axelle Lemaire vient d'être adoptée par une majorité de députés de l'Assemblée aujourd'hui. Sur 544 votants, 356 se sont prononcés en faveur de la nouvelle loi obtenant ainsi une large majorité.
Ainsi que la Secrétaire d'Etat chargée du Numérique l'avait énoncé devant l'Assemblée la semaine dernière, la loi est voulue construite selon la devise française, en trois axes :
• circulation des données et du savoir (liberté),
• protection dans la société numérique (égalité),
• l'accès des publics fragiles au numérique (fraternité).

Le gouvernement inscrit donc désormais dans le marbre législatif sa volonté de ne pas rater la vague de l'Open Data (Royaume-Uni, Danemark), tout en fournissant un nouveau cadre aux sites Internet et aux FAI (neutralité, loyauté des plates-formes).
Le vote a aussi permis de révéler que 187 votants se sont abstenus, la plupart des députés du groupe Les Républicains, avouant leur désapprobation de forme, et non de fond, du projet de loi dévoilé pour la première fois au début de l'été 2015.

Réagissez à cet article

Source : *La loi sur le numérique adoptée à 356 voix contre 1*

Fic 2016 : Etude d'impacts sur la vie privée : suivez la méthode de la CNIL

	**Fic 2016 : Etude d'impacts sur la vie privée : Suivre la méthode de la CNIL**

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.
Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :
• Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
• Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
• Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
• Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE

Réagissez à cet article

Source : *Etude d’impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l’informatique et des libertés*

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.

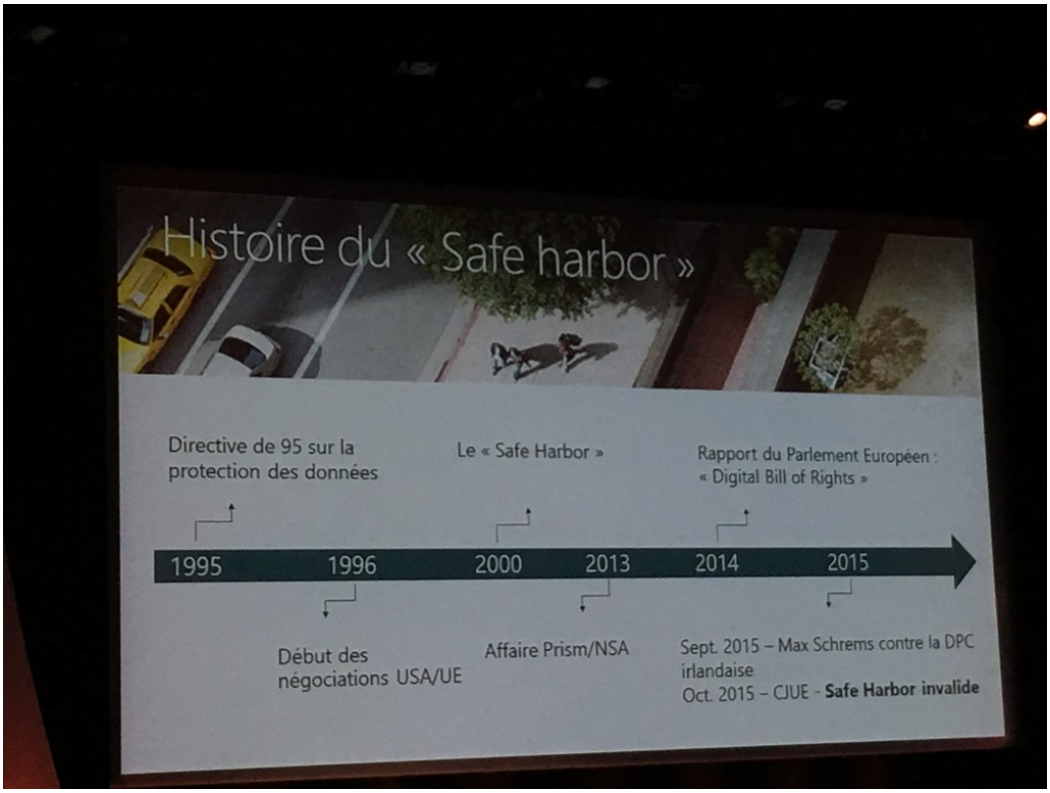
Réagissez à cet article

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

Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

	Fic 2016 : Comment mériter la confiance à l’heure de la remise en question du Safe Harbor

Le 6 octobre, la cours de justice de l'union européenne a invalidé le Safe Harbor. Cette session a pour but d'expliquer comment il est possible de mériter la confiance et de respecter la loi pour un fournisseur de service Cloud comme Microsoft.



Pour rassurer le groupe de travail de l'article 29, et pour venir compléter des mesures de sécurité se basant sur la norme iso 27001, plusieurs pistes ont été envisagées par Microsoft dont :
Faire appel à des contrôleurs de mises en conformité indépendants
S'engager à fournir la liste des sous-traitants…
Modifier ses conditions générales de ventes
S'engager à conserver confidentielles les données stockées hors cadre judiciaire

---

Réagissez à cet article

Source : *FIC 2016*

Ne donnez jamais une donnée personnelle de santé à un assureur

Ne donnez jamais une donnée personnelle de santé à un assureur

Quand il s'agit de données personnelles de santé, les Français ne doivent rien communiquer aux assureurs, aux banquiers ou aux employeurs. C'est le conseil de Philippe Douste Blazy, ancien ministre de la santé, et désormais créateur de la startup Honestica.

Les laboratoires pharmaceutiques à voir

Il a pris la parole lors de l'événement Keynote 2016 organisé par Maddyness le 20 janvier à Paris. "Il ne faut jamais donner de données personnelles aux assureurs, aux employeurs, aux banquiers," dit-il, "les laboratoires pharmaceutiques, il faut voir," ajoute-t-il.

Il parle alors de données personnelles. Il est plus ouvert pour l'usage de données de santé anonymisées. L'ancien ministre est revenu sur son expérience du dossier médical personnel. "Le DMP est le plus grand échec de ma vie quand j"étais ministre de la santé en 2004" déclare-t-il. Il croyait pourtant en ses vertus qu'il s'agisse d'accélérer les diagnostics, de détecter les risques liés à certains médicaments ou de réduire les coûts médicaux.

"En France, on dépense 30 milliards d'euros par an en examens redondants," pointe-t-il. "Vous vous blessez, on va vous faire faire une radio, et si vous devez aller à l'hôpital, on va refaire cette radio, on ne tient pas compte de la radio que vous avez faite dans le privé," illustre-t-il.

Mediator et sclérose en plaques

"Avec le DMP, on aurait vu en quelques mois et pas en années, que le Mediator créait des effets indésirables," souligne-t-il. "De plus, on avait dit que la vaccination contre l'hépatite B créait des risques de sclérose en plaques, on aurait vu que c'est faux grâce au DMP," martèle-t-il.

Depuis, il pense faire renaître ce dossier au sein de sa startup Honestica, où il est associé à Frank Le Ouay, l'un des cofondateurs de Criteo. "La création d'un dossier médical personnel a échoué chez les Américains parce qu'ils partent du patient, il faut partir du médecin, c'est lui qui dans le cadre de la relation de confiance avec le patient va pousser cette solution. Mais il faut lui vendre ce dossier médical comme un moyen de gagner du temps, une heure par jour, et pas comme de la paperasse supplémentaire," recommande-t-il.

Expérimentation en mars

Sa société va débuter l'expérimentation en mars prochain de sa solution auprès d'un hôpital toulousain. "Les comptes rendus de sortie de l'hôpital sont encore envoyés par la Poste," dit-il, "nous proposons de les gérer électroniquement." Et il mise sur les médecins hospitaliers pour faire le succès de ce dossier médical électronique.

Réagissez à cet article

Source : *Philippe Douste-Blazy : "ne donnez jamais une donnée personnelle de santé à un assureur" | La Revue du Digital*

Quels changements anticiper ? Le règlement européen sur les données personnelles annoncé pour le printemps :

	Quels changements anticiper Le règlement européen sur les données personnelles annoncé pour le printemps : ?

Ce règlement, dont le premier projet remonte à 2012, est appelé à remplacer la directive de 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ». Son objectif est d'uniformiser les règles en matière de protection des données personnelles en Europe, de garantir la libre circulation de ces données sur le territoire de l'Union et de simplifier l'exercice de leurs droits par les citoyens européens.

Après des débats parfois acharnés entre les acteurs en présence, que ce soit les CNIL européennes, les acteurs de l'internet et du Big-Data ou encore les représentants des consommateurs, une version consolidée a été arrêtée et diffusée le 15 décembre 2015.
De la loi du 6 janvier 1978 au futur règlement, la législation en matière de protection des données personnelles est allée dans le sens d'une complexité et d'une incertitude toujours plus grande. Les entreprises peuvent-elles attendre plus de sécurité juridique du futur règlement ? La réponse est contrastée.

Un projet de texte stabilisé… mais pas encore adopté
Il convient tout d'abord de tempérer l'enthousiasme affiché des institutions européennes : le texte définitif n'est pas encore adopté. Après un premier vote du Parlement européen en mars 2014, le Conseil de l'Union européenne donnait mandat au Luxembourg en juin 2015, dans le cadre de la présidence tournante de l'Union européenne, pour parvenir à un consensus sur le projet de règlement au plus tard fin décembre de la même année. Au terme de discussions intenses, Parlement et Conseil sont parvenus à un accord *in extremis* avant la trêve des confiseurs sur un document de pas moins de 200 pages…
Cet accord n'est pour le moment que politique, et la prochaine étape est un vote en deuxième lecture par le Parlement européen pour adoption définitive.
Le règlement européen sera ensuite applicable dans un délai de deux ans après son adoption. La différence essentielle par rapport à la directive de 1995 est que ce texte sera directement applicable au sein de l'Union européenne, sans que chacun des 27 états ne doive adopter des lois nationales de transposition, ce qui aurait nécessairement nui à l'objectif d'harmonisation. Les règles européennes nouvelles remplaceront donc automatiquement les règles nationales existantes incompatibles. Ainsi, pour ses 40 ans, la Loi française du 6 janvier 1978 dite « Informatique et Libertés » va se retrouver fortement vidée de sa substance.
Les entreprises ont donc encore un peu de temps devant elles pour se préparer à la mise en œuvre des nouvelles règles. Quels sont les changements majeurs à anticiper ?

***« Accountability »* et « *Privacy by Design* » sont des termes qui doivent devenir familiers**
Quelles données pourront être traitées ? Quelle durée de conservation appliquer ? Quels outils techniques installer ? Quelles formalités accomplir ?
Si le règlement uniformise la réponse à ses questions au sein de l'Union européenne… il ne les simplifie par nécessairement. Une large place sera faite à l'interprétation des dispositions nouvelles.

La **définition des données personnelles** ne change pas fondamentalement. Le règlement s'applique aux traitements des données identifiantes ou permettant d'identifier une personne, que ce soit directement ou indirectement. Le projet de règlement ajoute toutefois une série d'exemples de données qui permettent d'identifier une personne : son nom, mais également un numéro d'identification, une donnée de localisation, un identifiant d'un compte en ligne, ainsi que des références à des informations relatives à l'identité physique, génétique, mentale, économique, sociale ou culturelle d'une personne. Ces précisions sont dans la logique de la position actuelle des juridictions européennes et françaises.
S'agissant des **modalités de traitement** des données personnelles, il est abondamment fait référence dans le texte à la notion de *Privacy by Design*.
Qu'est-ce que cela signifie concrètement ? Les entreprises seront désormais tenues d'anticiper les sujets relatifs aux traitements de données dès les premières étapes de leurs projets informatiques, afin qu'il soit vérifié en amont que les développements à intervenir, où les logiciels à implémenter, seront conformes aux exigences imposées par le règlement.
Le responsable du traitement devra ainsi « *implémenter les mesures techniques et organisationnelles appropriées, telles que l'anonymisation, qui sont conçues pour mettre en œuvre les principes de protection des données, […] d'une manière effective et d'intégrer les protections nécessaires dans les traitements de manière à respecter les exigences du règlement et à protéger les droits des intéressés.* »
Une pondération devra en effet être faite entre coûts, état de l'art, contexte, finalités des traitements concernés, risques pour les droits et libertés des individus, etc. Autant de concepts dont la cohabitation laissera une grande place à une appréciation au cas par cas. Le règlement envisage qu'un mécanisme de certification soit mis en place, probablement afin de faciliter cette appréciation, bien que les procédures de certifications pèchent parfois par leur complexité.
Comme en l'état actuel de la législation, le règlement ne prévoit pas expressément de **durée de conservation des données**, et l'on peut le regretter. L'appréciation d'une durée de conservation des données sous une forme identifiante « *qui n'excède pas la durée nécessaire aux finalités pour lesquelles [les données] sont collectées et traitées* », place souvent le responsable de traitement dans une situation d'insécurité juridique. En revanche, dans sa dernière version, le projet de règlement prévoit que cette durée de conservation, ou *a minima* les critères retenus pour fixer cette durée, devront être portés à l'attention de la personne concernée dès la collecte. Les responsables de traitements devront donc apporter une attention particulière à ce sujet avant la mise en œuvre du traitement.
Les **formalités administratives** seront allégées : moins de notifications préalables aux autorités nationales, moins d'interlocuteurs. Un des objectifs principaux de ce texte est de garantir la libre circulation des données au sein de l'Union européenne. Ainsi, pour les groupes ayant des établissements dans plusieurs pays d'Europe, ou une activité ciblant plusieurs Etats-Membres, le principe du « guichet unique » permettra que les formalités requises ne soient effectuées qu'auprès de l'autorité de l'Etat Membre dans lequel le groupe a son établissement principal, les autorités des différents Etats Membres devant ensuite coopérer entre elles.
Les sociétés établies en dehors de l'Union européenne, mais ayant une activité ciblant le public européen, devront quant à elles désigner un représentant sur le territoire de l'Union, qui agira comme point de contact unique, tant pour les autorités que pour les personnes dont la société en question traite les données. A l'instar des pratiques en matière de fiscalité, cette dernière exigence incitera très probablement les grands acteurs du numérique non établis en Europe à désigner un représentant dans un Etat Membre dont l'autorité nationale de protection des données aura des règles réputées plus souples, ou disposera de moins de moyens pour diligenter des contrôles ou engager des procédures de sanction. Ces disparités devraient toutefois être tempérées par la coordination qu'assurera la nouvelle autorité européenne instaurée par le règlement.
En revanche, les **procédures internes seront quant à elles décuplées…** Un contrôleur à la protection des données devra être désigné dans les entités publiques et dans les entreprises traitant des données personnelles à une échelle importante. Il convient de souligner qu'il n'y a pas de seuil chiffré permettant à une entreprise de déterminer si elle doit ou non désigner une telle personne. Sa désignation est requise lorsque l'activité de l'entreprise implique le traitement de données personnelles de manière régulière et systématique sur une large échelle…
Le contrôleur pourra alternativement être salarié ou prestataire de service. Le responsable de traitement devra également tenir à jour des registres des traitements mis en œuvre sur le même modèle que ce qui existe actuellement pour les CIL. Dans la logique du principe d'« *accountability* », ces mesures devront permettre au responsable de traitement de démontrer que les traitements qu'il met en œuvre se font en conformité avec le règlement.
Afin de faciliter aux entreprises la mise en œuvre de telles procédures, et la démonstration de conformité du responsable de traitement à ses obligations, le règlement renvoie ici encore à un mécanisme de certification ou à des codes de conduite.

Et côté personnes physiques, quels droits ? Quelles protections nouvelles ?
Les personnes dont les données sont traitées devront bénéficier d'une **information plus large** sur les traitements qui les concernent. Outre les informations qui doivent déjà être fournies lors de la collecte de données en application de la Loi Informatique et Libertés, le responsable de traitement doit notamment préciser le fondement juridique du traitement, ainsi que la possibilité de déposer plainte auprès d'une autorité compétente d'un Etat Membre. Les mentions d'informations fournies par les responsables de traitement devront donc être ajustées.
Les personnes dont les données sont traitées bénéficieront d'un **droit à la portabilité de leurs données**. Les responsables de traitement devront donc être en mesure de restituer aux personnes dont les données sont traitées lesdites données, et ce dans un format standard et exploitable, afin qu'elles puissent être communiquées à un autre prestataire de services. Cette communication de données pourra même se faire directement au nouveau prestataire sur demande de la personne concernée.
Le projet de règlement prévoit des règles nouvelles encadrant **les traitements de données relatives aux enfants**. Ainsi, l'article 8 du projet de règlement prévoit une disposition visant à interdire aux services de la société de l'information destinés aux mineurs de 16 ans de recueillir leurs données personnelles sans autorisation préalable d'un titulaire de l'autorité parentale. Les Etats Membres pourront décider d'abaisser cette limite d'âge jusqu'à 13 ans. Le texte ajoute que le responsable de traitement devra fournir des efforts raisonnables, au regard des technologies disponibles, pour vérifier que le consentement est bien fourni par le titulaire de l'autorité parentale.
Les éléments détaillés ci-dessus ne sont que quelques points d'attention extraits parmi les 209 pages du projet de règlement dans sa dernière version. Les subtilités se cachent dans les détails et les 4 années de modifications et de reformulations du texte depuis sa première mouture ont pu altérer sa cohérence. Les deux années avant l'entrée en vigueur des dispositions nouvelles ne seront pas de trop pour permettre aux entreprises de se mettre en conformité. D'autant qu'en cas de manquement, les sanctions administratives pourront désormais aller jusqu'à 20 000 000 d'euros ou 4% du chiffre d'affaires mondial… ce qui est sans commune mesure avec les 150 000 euros d'amende que peut à ce jour prononcer la CNIL.

Réagissez à cet article

Source : *Le règlement européen sur les données personnelles annoncé pour le printemps : Quels changements anticiper ? – Féral-Schuhl Sainte-Marie*