Futur Règlement européen sur la protection des données, qui est concerné ?

Futur Règlement européen sur la protection des données, qui est concerné ?

Le 25 février dernier, Arendt & Medernach organisait une conférence sur le futur Règlement européen sur la protection des données (ci-après « le Règlement »[1]afin de permettre aux entreprises de mieux comprendre les nouvelles obligations auxquelles elles seront prochainement soumises et leur procurer l'essentiel de ce qu'il faut retenir de ce nouveau texte.

Contexte

Après deux années riches en actualités en matière de données personnelles (droit à l'oubli consacré par la Cour de Justice de l'Union européenne (CJUE)[2], et invalidation du Safe Harbor[3] notamment), le nouveau Règlement arrive à point nommé pour remplacer le cadre juridique actuel adopté il y a plus de 20 ans[4].

4 ans de discussions et 4000 amendements ont été nécessaires pour parvenir à un accord autour de ce nouveau texte qui sera adopté en mai/juin prochain. Il sera applicable dans deux ans à compter de sa date d'entrée en vigueur, soit pour l'été 2018.
Si l'échéance semble lointaine, il est toutefois nécessaire d'envisager dès à présent les changements apportés par ce nouveau texte.

De nouvelles obligations pour les entreprises

Il résulte de ce Règlement diverses obligations pour les entreprises et notamment :

• De mettre en œuvre les principes de « privacy by design / privacy by default» afin d'assurer une protection des données dès leur conception et par défaut ;
• De tenir des registres des traitements de données personnelles sauf cas exceptionnels ;
• De notifier toute violation de données dans les 72h auprès de l'autorité de contrôle voire de la personne concernée le cas échéant ;
• De détailler/préciser l'information des personnes concernées ;
• D'adapter leurs contrats de sous-traitances ;
• D'assurer la portabilité des données ;
• De nommer un Délégué à la Protection des Données le cas échéant.
• Les entreprises doivent envisager ces obligations avec le plus grand sérieux puisque de nouvelles sanctions financières pourront désormais être prononcées par les autorités nationales de protection des données. En effet, selon le manquement, ces sanctions pourront atteindre de 2 à 4% du chiffre d'affaires mondial d'une entreprise ou de 10 à 20 millions d'euros, le montant le plus important devant être retenu.

Qu'est-ce qu'une donnée personnelle ?

"Les données à caractère personnel sont définies par le futur Règlement comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement , notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale ».
Cette définition est identique à celle prévue actuellement dans la loi luxembourgeoise[7] mais elle ajoute quelques exemples. Il est notamment précisé qu'un identifiant en ligne, tel qu'une adresse IP, peut être qualifié de données à caractère personnel," explique Héloïse Bock, Partner Arendt & Medernach.

Est-ce qu'on peut dire que toutes les entreprises seront concernées par ce nouveau Règlement ?

"Le champ d'application du règlement est élargi puisque celui-ci aura vocation à s'appliquer à toutes les entreprises traitant des données personnelles dès lors qu'elles sont établies sur le territoire de l'Union européenne ou, lorsqu'elles sont établies hors de l'Union européenne si ces traitements ciblent des citoyens européens.
Un grand nombre d'entreprises seront ainsi concernées en pratique," poursuit-elle.

Des droits nouveaux et renforcés

Pour les personnes concernées, ce nouveau Règlement introduit le célèbre droit à l'oubli ou droit à l'effacement, déjà consacré par la CJUE en 2014[5] mais également, le droit à la portabilité des données qui permet de transférer les données d'un prestataire vers un autre. Les droits d'accès, d'opposition et de rectification des données ainsi que le droit à l'information, existants dans le cadre juridique actuel, sont maintenus et renforcés.

Les transferts de données hors de l'Union européenne

Concernant les transferts de données en dehors de l'Union européenne, le Règlement ajoute de nouvelles bases de légitimité ponctuelles/limitées sur lesquelles un responsable de traitement pourra se fonder en cas de transfert vers un pays n'assurant pas un niveau de protection adéquat.
Le sort des transferts de données réalisés vers les Etats-Unis n'est pas réglé par le Règlement, toutefois, une nouvelle décision d'adéquation est attendue très prochainement[6]. La Commission européenne et les États-Unis se sont en effet accordés sur un nouveau cadre pour les transferts transatlantiques de données le mois derniers : le «bouclier vie privée UE-États-Unis» ou « EU-US Privacy Shield ».

To do list avant 2018

Pour conclure, les avocats d'Arendt & Medernach ont dressé une « to do list » générale reprenant les points suivants :

• Recenser les traitements de données réalisés en pratique et leurs finalités;
• Faire un audit pour évaluer le niveau de conformité actuel et identifier les lacunes;
• Réaliser un « mapping » de tous les transferts de données en considérant les catégories de données, les destinataires des transferts, les bases de légitimité etc.;
• Effectuer des études d'impact lorsqu'un traitement à risque est envisagé;
• Nommer un délégué à la protection des données si nécessaire;
• Mettre en place ou adapter la documentation existante (registres, policies, contrats de sous-traitance, etc.)

[1] Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (2012/0011 COD)
[2] CJUE, 13 mai 2014, affaire C-131/12
[3] CJUE, 6 octobre 2015, affaire C-362/14
[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 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
[5] CJUE, 13 mai 2014, affaire C-131/12
[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
… [Lire la suite]

Réagissez à cet article

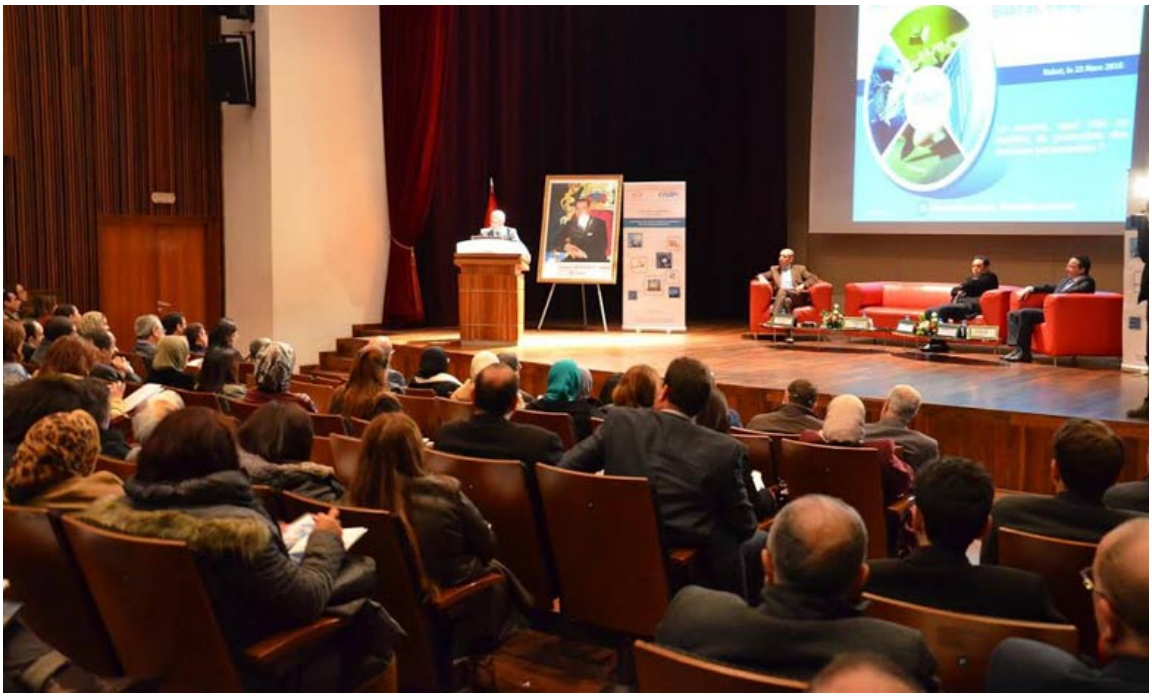
Source : *Futur Règlement européen sur la protection des données, qui est concerné ?*

Les notaires marocains sensibilisés à la protection des données personnelles

Les notaires marocains sensibilisés à la protection des données personnelles

---

L’accent a été mis sur les dispositions de la loi 09-08, mais aussi sur le rôle et les missions de la Commission nationale de contrôle de la protection des données à caractère personnel.



Les notaires ont été invités le 23 mars dernier, à prendre part à un séminaire placé sous le thème «Le notaire, quel rôle en matière de protection des données personnelles ?».

La rencontre organisée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), en partenariat avec le Conseil national de l’ordre des notaires du Maroc (CNONM) avait pour but de mettre la lumière sur les dispositions de la loi 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel, mais aussi sur le rôle et les missions de la CNDP.

Ainsi, les notaires ont eu l’occasion de mieux appréhender les enjeux liés à la protection des données personnelles dans l’exercice de leur mission. Le séminaire leur a aussi permis de situer leur rôle dans la consécration des droits des citoyens à la protection de la vie privée et des données personnelles, et de prendre connaissance des obligations légales en vigueur.

Les deux organisateurs soulignent, par ailleurs, que cette initiative «constitue également un premier pas vers une coopération plus étroite entre la CNDP et le Conseil national de l’ordre des notaires»… [Lire la suite]

Réagissez à cet article

Source : *:: Le Matin :: Les notaires sensibilisés à la protection des données personnelles*

Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Le principe d'«Accountability » n'est pas nouveau dans le domaine de la protection des données et de la vie privée. Plusieurs textes y ont déjà fait référence et notamment les lignes directrices émises par l'OCDE en 1980, le Standard de la conférence Internationale de Madrid, la norme ISO 29100 ou les règles mises en place au sein de l'APEC. Au sein même de la directive 95/46, le possible recours aux règles internes de groupe pour encadrer les transferts de données en dehors de l'Union Européenne, reflètent cette notion qui vise à responsabiliser le responsable de traitement.

Comment définir le principe d'«Accountability » ?

Ce terme est difficile à traduire en français. Cela revient à montrer comment le principe de responsabilité est mis en œuvre et à le rendre vérifiable. Il est souvent traduit en français par l'« obligation de rendre compte ».
Pour le G29[1] , cela doit s'entendre comme des « mesures qui devraient être prises ou fournies pour assurer la conformité en matière de protection des données ».

Le principe d'«Accountability » dans le Règlement Général de Protection des Données

La traduction française du texte, à savoir « le principe de responsabilité », ne reflète pas toute la signification de ce terme. C'est en lisant le détail des dispositions du règlement, que l'on en saisit la portée.
– Le responsable du traitement est responsable du respect des principes (i.e.de la licéité, de la loyauté, de la transparence des traitements, du respect du principe de finalités, de minimisation des données, de l'exactitude des données, du respect de la durée de conservation et des mesures de sécurité) ;
– Et il est en mesure de démontrer que ces dispositions sont respectées. A cet effet, l'article 22 du Règlement précise que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné aux activités de traitement de données, les mesures comprennent la mise en œuvre de politiques appropriées.
– Comme dans tout processus d'amélioration continue, ces mesures doivent être réexaminées et actualisées si nécessaire.

Qui est soumis au principe d'« Accountability » ?

Selon les dispositions de l'article 5 du règlement européen, ce principe concerne le responsable de traitement.
Les sous-traitants auront eux aussi des responsabilités portant sur la mise en œuvre de mesures ou sur la documentation des traitements ; mais si le vocabulaire utilisé dans le texte du règlement est souvent similaire, il ne semble pas que l'on puisse en déduire que les sous-traitants seront soumis au respect du principe d'« Accountability ».
Il en va probablement différemment du représentant qui agit pour le compte et au nom du responsable de traitement établi en dehors de l'Union Européenne et qui de ce fait, doit remplir les obligations qui lui incombent.

De quelles mesures technique et organisationnelles s'agit-il ?

Ces mesures doivent être prise en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes.
Le G29 précise que la mise en pratique du principe d' « Accountability » suppose une analyse au « cas par cas ».
L'article 23 du Règlement relatif à la protection des données dès la conception et par défaut, précise que le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à donner effet aux principes de protection des données et notamment à la minimisation.
Il est par ailleurs indiqué à l'article 28 du Règlement, que chaque responsable du traitement tient un registre décrivant les traitements et dans la mesure du possible, les mesures de sécurité techniques et organisationnelles mise en place.
Selon l'article 30 du Règlement européen, le responsable de traitement est tenu de prendre des mesures de sécurité et notamment selon les besoins :
– la pseudonymisation et le cryptage des données à caractère personnel ;
– des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données ;
– des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci (…) en cas d'incident ;
– une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité.

Les mesures indiquées dans le Règlement Européen font écho à celles citées en exemple par le G29 à l'occasion de son avis[2] émis sur l'« Accountability »:
– Des politiques et procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création ou la modification d'un traitement),
– L'inventaire des traitements,
– La répartition des rôles et responsabilités,
– La sensibilisation et formation du personnel,
– La désignation d'un délégué à la protection des données,
– La vérification de l'efficacité des mesures (contrôles, audits).

Lors de la 31ème Conférence des Commissaires à la Protection des Données et à la Vie Privée de Madrid, le principe d'«Accountability » avait été illustré de la manière suivante:
– Implémentation de procédures destinées à prévenir et détecter les failles,
– La désignation d'un ou de plusieurs délégués à la protection des données,
– Des sessions de sensibilisation et de formation régulières,
– La conduite régulière d'audits indépendants,
– La prise en compte de la réglementation au travers de spécificités techniques,
– La mise en place d'études d'impacts sur la vie privée,
– L'adoption de codes de conduite.
Le G29 a également indiqué que la transparence sur les politiques de confidentialité et sur la gestion interne des plaintes contribuait à un meilleur niveau d'« Accountability ».

Le rôle de la certification

Le Règlement européen précise que l'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à attester du respect des obligations incombant au responsable du traitement au titre de l' « Accountability ».
De manière générale, les actes délégués de la Commission devraient fournir de plus amples informations sur le sujet.

Le principe d'« Accountability » : une évolution plus qu'une révolution

L'« Accountability » n'est pas une révolution dans la mesure où les organisations ont déjà l'obligation de se conformer aux principes de protection des données et notamment à la loi Informatique et Libertés en France. Ce principe est d'ailleurs déjà connu des acteurs du secteur financier.
L'obligation de documentation à des fins de démonstration est en revanche plus novatrice et ce d'autant plus que les entreprises connaissent mal l'étendue de cette réglementation.
Ainsi en cas de violation des principes de protection des données, les autorités de protection des données devraient prendre en considération l'implémentation (ou pas) de mesures et l'existence de procédures de contrôle.
De plus, si les informations relatives aux procédures et politiques ne peuvent être fournies, les autorités de protection des données pourront sanctionner une organisation sur la base de ce seul manquement, indépendamment du fait qu'il y ait eu une violation des données.
Comme l'a indiqué le groupe de travail des autorités européennes de protection des données (G29), les personnes ayant des connaissances techniques et juridiques pointues en matière de protection des données, capables de communiquer, de former le personnel, de mettre en place des politiques et de les auditer seront indispensables à la protection des données.
[1] Opinion 3/2010 on the principle of accountability
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
… [Lire la suite]

Réagissez à cet article

Source : *Règlement Européen de Protection des Données Personnelles : Le principe d'« Accountability » ou comment passer de la théorie à la pratique – CIL Consulting*

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

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

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

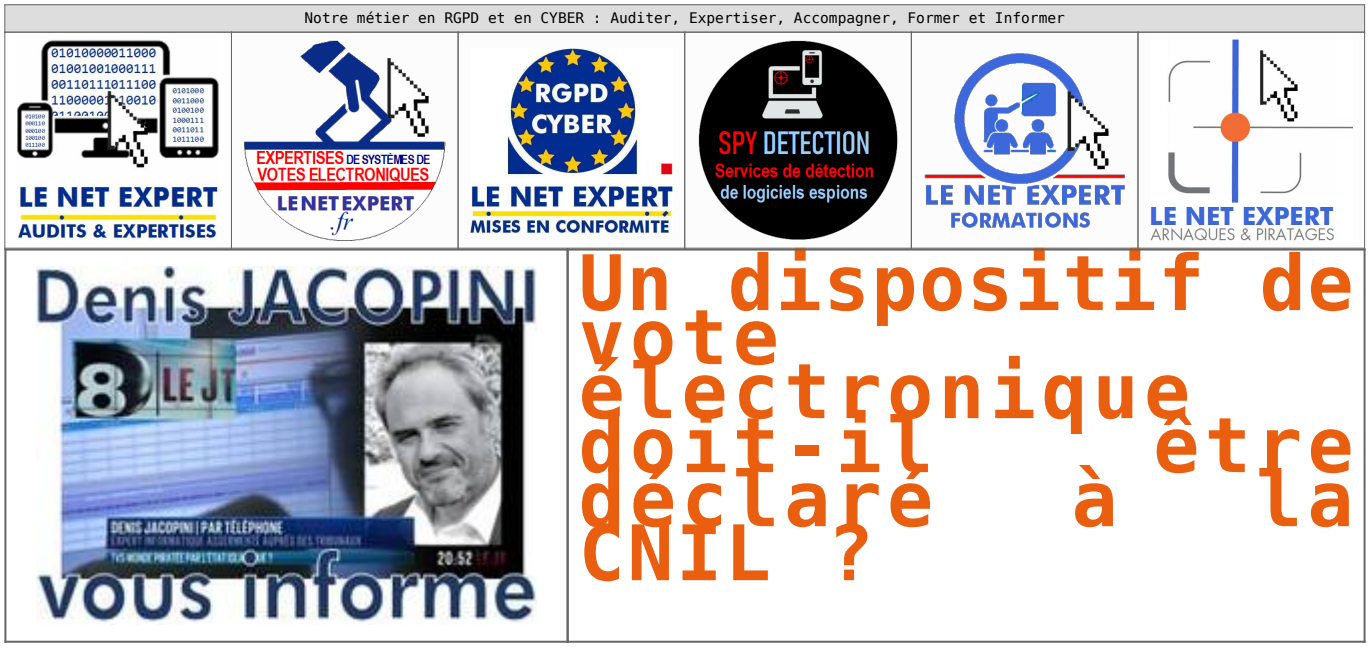
Le cadre était attendu depuis l'annulation du Safe Harbor par la Cour de justice de l'UE (CJUE) dans son arrêt du 6 octobre 2015, qui avait créé un vide juridique important en matière de transfert des données (voir notre article).
La Commission européenne et le groupe des CNIL européennes (G29) avaient,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

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

Réagissez à cet article

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

Un dispositif de vote électronique doit-il être déclaré à la CNIL ?



Un dispositif de vote électronique, notamment pour l'organisation d'élections primaires, doit être déclaré à la CNIL et répondre aux recommandations n° 2010-371 formulées par la Commission.

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

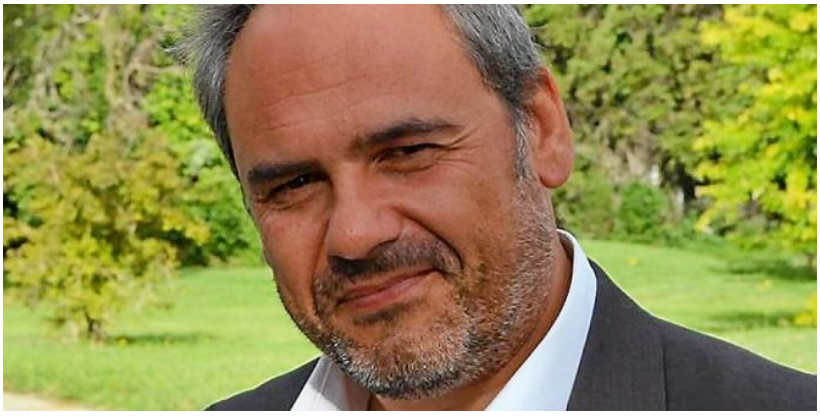
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise



Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

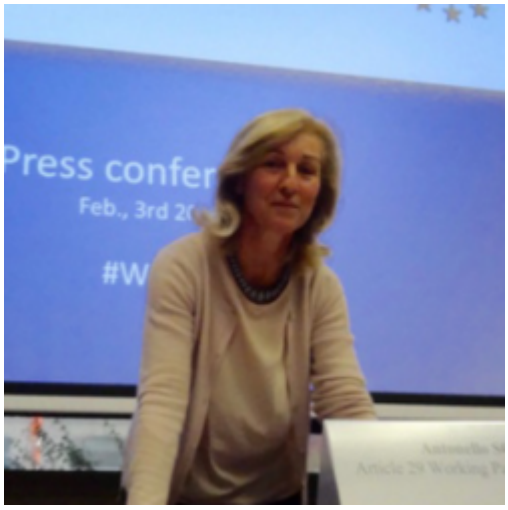
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *CNIL Besoin d'aide ? – Vote électronique : le dispositif doit-il être déclaré à la CNIL ?*

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



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

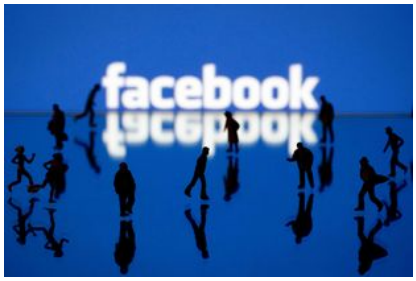
La Commission Nationale de l'Informatique et des Libertés a publiquement mis en demeure Facebook de ne plus placer de cookies indésirables sur les postes des utilisateurs et d'arrêter le transfert des données personnelles de ses membres vers les Etats-Unis.

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

Réagissez à cet article

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

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 ».

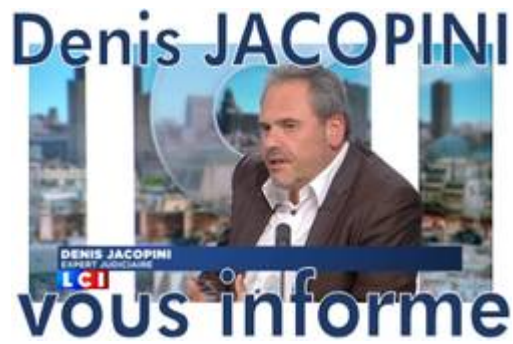
Cependant, en dépit des efforts réalisés par les Etats-Unis, il réitère ses préoccupations concernant les nécessaires garanties à apporter.
Ainsi, dans son communiqué de presse en date du 3 février 2016 (1), le groupe de travail de l'article 29 rappelle, sur le fondement de la jurisprudence européenne, 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 ».

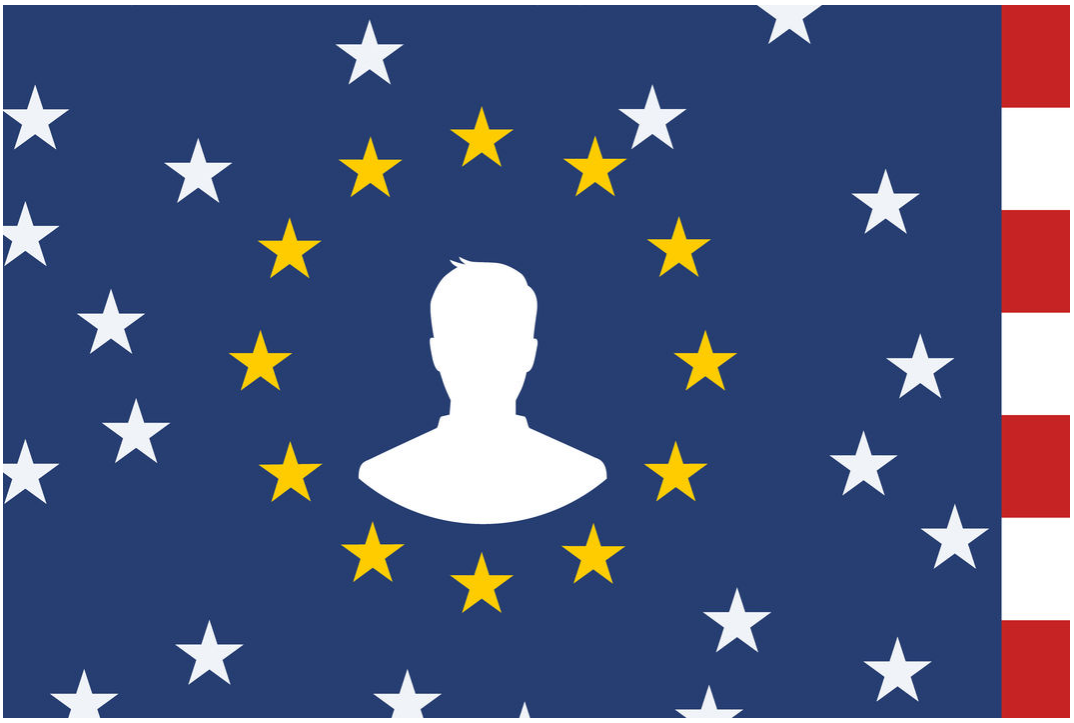
Il protégera les « droits fondamentaux » des Européens, a assuré la commissaire européenne chargée de la Justice, Vera Jourova, et donnera aux entreprises « la sécurité juridique dont elles ont besoin », a appuyé son collègue Andrus Ansip, responsable du numérique, lors d'une conférence de presse à Strasbourg.
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*