Du *Safe Harbor* au *Privacy Shield*

Les soubresauts législatifs et jurisprudentiels liés au transfert des données personnelles hors de l'Union européenne

Les révélations d'Edward Snowden et les dénonciations sur les pouvoirs exorbitants des agences de renseignement américaines, via le *Patriot Act*, ont conduit à invalider l'accord du *Safe Harbor* pour les échanges transatlantiques de données à caractère personnel vers les États-Unis. Deux ans ont été nécessaires pour que la Commission et les autorités américaines parviennent à un nouvel accord : le « *EU-US Privacy Shield* ». Celui-ci suscite toutefois encore de nombreux débats, représentatifs des difficultés à mettre en œuvre des transferts de données transfrontières depuis ces dernières années.

MARIE ABADIE*
Directrice des affaires juridiques

Microsoft France

*avec la participation de Mathilde Fouillard, juriste, Microsoft, et Étienne Lagier, *Contract Manager*, Microsoft.

Le transfert de données personnelles n'est pas défini par la directive 95/46CE 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 des données) ni dans la loi informatique et libertés du 6 janvier 1978.

Toutefois, le guide de la CNIL sur le transfert de données[1] parle de « *transfert lorsque les données à caractère personnel sont transférées depuis le territoire européen vers un ou des pays situés hors de l'Union européenne [UE]. Le transfert peut s'effectuer par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre* ». Un transfert de données au sens de la réglementation française et européenne concerne donc aussi bien un hébergeur de données qu'un prestataire de maintenance qui visualiserait la donnée depuis l'Inde par exemple.

Le transfert en dehors de l'UE est donc interdit, sauf s'il s'opère sur des bases légales adéquates. La personne a donné son consentement de manière explicite et sans ambiguïté ou le transfert a été nécessaire notamment : pour des raisons d'intérêt vital pour la personne, lorsqu'un contrat existe entre le responsable de traitement et la personne, pour la sauvegarde de l'intérêt public ou pour l'exercice ou la défense d'un droit en justice.

Le transfert est également possible vers un pays tiers, s'il existe des garanties de protection adéquates : des règles internes d'entreprise (*Binding Corporate Rules*) ou des clauses contractuelles types de l'UE.

Enfin, on se souviendra que parmi les moyens ou véhicules juridiques permettant de transférer des données hors de l'Europe, la directive 95/46 du 24 octobre 1995 (*Journal Officiel* n° L 281 du 23 novembre 1995, pp. 31-50), 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 avait prévu la possibilité pour les États vers lesquels des données étaient transférées de signer une convention avec l'UE. Ce fut le cas pour les États-Unis qui signèrent l'accord du *Safe Harbor* en 2000 avec la Commission européenne (Décision 2000/520/EC/July 2000).

Toutefois, Max Schrems, étudiant autrichien, avait déposé une plainte contre le réseau social amé-

1. https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf / novembre 2012.

ricain Facebook, suite aux révélations d'Edouard Snowden sur le programme Prism permettant aux agences de renseignements américains d'avoir un accès privilégié aux données des Américains et des Européens.

Cette violation devait, selon lui, être sanctionnée par le Commissaire à la protection des données de l'Irlande (*Data Protection Commissioner* – DPC). Cette dernière avait toutefois refusé de se prononcer sur la validité du *Safe Harbor*.

La Haute Cour irlandaise saisie de cette affaire renvoyait celle-ci devant la Cour de Justice de l'Union européenne (CJUE) qui invalidait le *Safe Harbor* le 6 octobre 2015 (CJUE 6 octobre 2015, affaire C-362/14, *Maximilian Schrems c/Data Protection Commissionner*).

Avant de comprendre les évolutions jurisprudentielles et législatives outre-Atlantique liées à la protection sur la vie privée, il nous a semblé intéressant de revenir sur les raisons qui ont fait couler tant d'encre depuis plusieurs années.

I. RAPPEL DES DÉSÉQUILIBRES ENTRE VIE PRIVÉE ET INTÉRÊT NATIONAL DÉNONCÉS PAR LES JUGES DE LA CJUE

Dans le cadre de la décision *Schrems* du 6 octobre 2015, la CJUE avait considéré, pour invalider le *Safe Harbor*, qu'« *une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant* » atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte des droits fondamentaux de l'UE (« *Toute personne a droit au respect de sa vie privée et familiale de son domicile et de ses communications* »).

La Cour pointait également le fait que les citoyens européens ne disposaient d'aucun recours pour protester contre l'utilisation de leurs données personnelles aux États-Unis en violation de la législation européenne et devaient avoir le droit de bénéficier d'une protection juridictionnelle effective.

Par ailleurs, les juges considéraient que la Commission « *était tenue de constater que les États-Unis assurent effectivement un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union* » et lui reprochaient de ne pas l'avoir fait. Il est rappelé par la CJUE que les autorités de protection des données nationales ont non seulement le droit, mais aussi l'obligation, d'examiner au cas par cas chaque plainte de citoyen de l'UE qui remettrait en cause le niveau de protection assuré dans le cadre de transferts de données personnelles.

Le 2 février 2016, après deux années de négociations, la Commission et le ministère du Commerce américain (« *Department of Commerce* ») sont parvenus à un accord politique sur un nouveau cadre pour les échanges transatlantiques de données à caractère personnel à des fins commerciales vers les États-Unis : « *EU-US Privacy Shield* » ou « *le bouclier de protection des données UE-US* ». Conformément à l'article 25(2) de la Directive 95/46/EC, la Commission européenne adoptait 12 juillet 2016 une décision d'adéquation visant à reconnaître au mécanisme susvisé un niveau de protection « *essentiellement équivalent* » aux exigences européennes, notifiée aux États membres de l'UE le même jour et entrant en vigueur à compter de sa notification.

II. LES RÉPONSES DES AUTORITÉS AMÉRICAINES

Au fil du temps et plus particulièrement après les révélations d'Edward Snowden et des différentes dénonciations sur les pouvoirs exorbitants dont étaient dotées les agences de renseignement américaines via le *Patriot Act*, texte renforçant l'arsenal juridique américain existant en cas de terrorisme, on a pu constater une évolution des décisions des représentants des pouvoirs exécutif, législatif et judiciaire.

Lors de la négociation du *Privacy Shield*, le Gouvernement américain a pu rappeler le dispositif existant permettant d'encadrer l'exercice des agences de renseignements en cas d'accès aux données personnelles.

1. Le pouvoir exécutif

1.1. La PPD-28

Lors de la revue du *Privacy Shield* et des différents échanges avec la Commission européenne, le Gouvernement américain rappelait que le 17 janvier 2014, le président américain avait bien pris une « *Policy Directive* » encadrant les opérations de renseignement.

En effet, comme indiqué au considérant 74 de la décision, validant le *Privacy Shield*, il est clairement précisé que la PPD 28 restreint l'utilisation des données « en vrac » à six motifs spécifiques de protection de la sécurité nationale : « *même dans les cas où les États-Unis jugent nécessaire de recueillir des renseignements d'origine électromagnétique en vrac, dans les conditions fixées aux considérants 70 à 73, la PPD-28 restreint l'utilisation de ces renseignements à une liste spécifique de six motifs de protection de la sécurité nationale, en vue de défendre la vie privée et les libertés civiles de toutes les personnes, quels que soient leur nationalité et leur lieu de résidence. Ces motifs autorisés comprennent des mesures visant à (1) détecter et à neutraliser les menaces liées à l'espionnage, (2) au terrorisme et (3) aux armes de destruction massive, (4) les menaces pour la cybersécurité, ainsi que (5) les menaces contre les forces armées ou le personnel de l'armée et (6) les menaces criminelles transnationales liées aux cinq autres motifs ; ils seront réexaminés au moins une fois par an. Selon les observations des autorités américaines, les acteurs de la communauté du renseignement ont renforcé leurs pratiques et normes analytiques en matière d'interrogation de données de renseignement d'origine électromagnétique non évaluées de façon à se conformer à ces exigences ; l'utilisation de questions ciblées garantit que seules les informations dont on estime qu'elles présentent un intérêt potentiel du point de vue du renseignement sont soumises pour examen aux analystes.* »

1.2. Les États-Unis se sont aussi dotés d'une « *Privacy and Civil Liberties Oversight Board* »

Ce Comité a pour rôle de s'assurer que les efforts de lutte contre le terrorisme par le Gouvernement soient équilibrés au regard des libertés civiles et de protection de la vie privée. Ce Comité indépendant au

sein de l'exécutif est composé de membres nommés par le président avec l'approbation du Sénat. Il peut accéder à tous les dossiers, rapports, vérifications, examens, documents, documents et recommandations pertinents de l'organisme, y compris les renseignements classifiés, effectuer des entrevues et entendre des témoignages. Il évaluera la mise en œuvre de la PPD-28.

1.3. Le Bureau de surveillance du renseignement

Ce dernier est établi au sein du Conseil consultatif du renseignement du président veille au respect de la Constitution par les autorités de renseignement américaines de la Constitution et de toutes les règles applicables.

La Commission européenne souligne que « *ces mécanismes garantissent que la question sera abordée au plus haut niveau de la communauté du renseignement. Lorsqu'il s'agit d'une personne non américaine, le directeur du renseignement national, en consultation avec le Secrétaire d'État et le chef du service ou de l'organisme notifiant, détermine si des mesures doivent être prises pour aviser le gouvernement étranger concerné, conformément à la protection de sources et de méthodes et du personnel américain* » (considérant 85).

Enfin, les activités de renseignement menées par les autorités publiques américaines sur la base du *FISA Act* permettent le réexamen et, dans certains cas, requièrent l'autorisation préalable de la FISC, tribunal indépendant dont les décisions peuvent être contestées avant la Cour d'examen des renseignements étrangers (FISCR) et la Cour suprême des États-Unis. Les droits de recours individuels, dans le cadre de la surveillance américaine peuvent porter sur : l'ingérence de la NSA, l'accès illicite et intentionnel aux données à caractère personnel par des fonctionnaires et l'accès à l'information en vertu de la loi sur la liberté d'information (FOIA).

1.4. La signature du *Privacy Shield* et ses garanties associées

Le *Privacy Shield* est un mécanisme qui permet aux entreprises ou aux particuliers de garantir le droit fondamental à la protection de leurs données personnelles lorsqu'elles sortent de l'UE vers les États-Unis et sont confiées à des sociétés américaines.

Il faut pour cela que la société américaine s'enregistre auprès du Département du commerce (ou *Department of Commerce* – DoC) américain. Ce dernier est responsable de gérer les conditions d'application de ce mécanisme. Les sociétés y adhérant doivent avoir une politique de protection des données personnelles en ligne avec les principes du *Privacy Shield*. Leur adhésion doit être renouvelée chaque année.

a. Les engagements des entreprises adhérentes aux principes du Privacy Shield

Les entreprises américaines étant susceptibles de traiter des données personnelles des citoyens européens devront respecter sept principes clés :
– elles devront fournir aux citoyens concernés les informations nécessaires concernant les données collectées (principe de notification), et notamment les catégories de données, les raisons de leur traitement, leur droit d'accès, à qui s'adresser auprès de la société en cas de réclamation, la possibilité pour l'entreprise de devoir répondre à des requêtes légales d'autorités publiques pour communiquer des informations.
– elles devront également leur laisser le choix de ne pas communiquer leurs données personnelles à des tiers, mais également de choisir que leurs données ne soient pas utilisées dans un but « *matériellement différent* » (principe de choix) de celui convenu initialement. Toutefois, il est admis par exemple que si les données personnelles d'un employé européen sont transférées aux États-Unis à la maison mère américaine, cette dernière peut réutiliser ces données pour lui adresser une offre d'une nouvelle société d'assurance ou d'un fonds de pension sans avoir à obtenir le consentement de l'employé ;
– par ailleurs, elles devront mettre en place des mesures de sécurité raisonnables et appropriées pour la protection des données personnelles et s'assurer que leurs sous-traitants respectent ces mêmes mesures (principe de sécurité) ;
– la collecte de données personnelles doit être limitée à ce qui est pertinent dans le cadre du traitement et les entreprises ne doivent pas traiter des données personnelles dans un but incompatible avec celui pour lequel la collecte avait eu lieu (principe de l'intégrité de la donnée) ;
– les citoyens européens ont un droit d'accès aux données personnelles collectées, et ainsi un droit de correction et de suppression de ces données si elles vont à l'encontre des principes de protection de la vie privée (principe d'accès) ;
– tout transfert ultérieur de données personnelles ne peut avoir lieu que dans un but limité et spécifique et sur la base d'un contrat qui prévoit les mêmes niveaux de protection (principe de responsabilité pour les transferts ultérieurs) ;
– enfin, des mécanismes efficaces de recours pour les citoyens de l'UE doivent être mis en place en cas de non-conformité avec les principes du *Privacy Shield* (principe de recours et de responsabilité).

b. Les limites sur la collecte de masse

La décision ayant mis en place le *Privacy Shield*, prévoit que :
– « *les composantes de la communauté du renseignement* [des États-Unis] *doivent parfois collecter des renseignements d'origine électromagnétique en vrac dans certaines circonstances, par exemple pour détecter et évaluer les nouvelles menaces ou les menaces émergentes. […] Il s'ensuit que la collecte en vrac n'aura lieu que lorsque la collecte ciblée au moyen de discriminants – c'est-à-dire un identifiant associé à une cible spécifique (tel que l'adresse électronique ou le numéro de téléphone de la cible) – n'est pas possible "pour des raisons techniques ou opérationnelles". Cela vaut tant pour la manière dont les renseignements d'origine électromagnétique sont collectés que pour les renseignements qui sont effectivement collectés* » (considérant 72) ;
– « *lorsque la communauté du renseignement* [des États-Unis] *ne peut pas utiliser des identifiants spécifiques pour cibler la collecte, elle s'efforcera de réduire "autant que possible" le champ de la collecte. Afin de respecter ce principe, elle "applique des filtres et d'autres moyens techniques pour focaliser la collecte sur les dispositifs qui sont les plus susceptibles de contenir des informations présentant un intérêt pour*

le renseignement extérieur" [et elle répondra donc aux exigences élaborées par les décideurs politiques américains conformément au processus décrit ci-dessus, au considérant 70]. En conséquence, la collecte en vrac sera ciblée au moins de deux façons, comme indiqué ci-après. Premièrement, cette collecte portera toujours sur des objectifs liés au renseignement extérieur (par exemple, pour acquérir des renseignements d'origine électromagnétique sur les activités d'un groupe terroriste opérant dans une région donnée) et sera toujours focalisée sur les communications qui présentent un tel lien. Selon les assurances données par l'ODNI, cela est illustré par le fait que les "activités de renseignement d'origine électromagnétique menées par les États-Unis ne touchent qu'une faible partie des communications transitant sur internet". Deuxièmement, les observations de l'ODNI expliquent que les filtres et autres moyens techniques utilisés seront conçus de manière à cibler la collecte "aussi précisément que possible" de façon à garantir que le volume de "données non pertinentes" soit réduit au minimum » (considérant 73) ;

– « *la priorité est clairement donnée à une collecte ciblée, tandis que la collecte en vrac est limitée aux situations (exceptionnelles) dans lesquelles une collecte ciblée n'est pas possible pour des raisons techniques ou opérationnelles* » (considérant 76).

c. Les recours gracieux

Le *Privacy Shield* n'a pas seulement pour vocation de rappeler les grands principes de protection des données à suivre lors du traitement de données à caractère personnel de citoyens européens. L'un des principaux apports de cette décision, et qui veut en cela se démarquer fondamentalement du *Safe Harbor*, est la création de voies de recours plus efficaces en cas de violation des principes posés. Bien que les modalités pratiques de ces recours soient encore, pour certaines, en cours d'élaboration, les options possibles sont toutefois connues.

Les personnes dont les données sont traitées par une entreprise américaine auto-certifiée au titre du *Privacy Shield* peuvent en premier lieu s'adresser directement à cette entreprise, laquelle doit désigner un point de contact en cas de question ou de réclamation. En pratique, ce point de contact sera indiqué dans la politique de confidentialité de l'entreprise, généralement mise à disposition par le biais de son site internet. À réception d'une réclamation, une réponse doit être apportée sous quarante-cinq jours par l'entreprise, en indiquant si la réclamation est fondée ainsi que les mesures prises pour remédier au problème soulevé, le cas échéant.

Si le litige n'est pas résolu, le *Privacy Shield* impose aux entreprises adhérentes de proposer un mécanisme de recours indépendant. Ce mécanisme peut prendre la forme soit d'un organisme de règlement extrajudiciaire des litiges (*Alternative Dispute Resolution* – ADR), soit d'une soumission volontaire de la réclamation au contrôle d'un panel d'Autorités européennes chargées de la protection des données (*Data Protection Authorities* – DPA).

S'il est fait le choix d'un mécanisme d'ADR[2], l'organisme choisi et la procédure pour formuler une réclamation doivent être communiqués à la personne concernée, par exemple via le site internet de l'entreprise. De même, l'organisme désigné doit lui-même fournir des détails sur le fonctionnement du *Privacy Shield* et sur la procédure à suivre sur son propre site internet, ainsi qu'un rapport annuel fournissant des statistiques sur le traitement des réclamations. Cet organisme peut être situé aux États-Unis ou dans l'UE, au choix de l'entreprise. En toute hypothèse, la procédure doit demeurer gratuite pour la personne à l'origine de la réclamation.

S'il est plutôt fait le choix de se soumettre volontairement au contrôle du panel de DPA européennes[3], ce panel doit adresser un avis au plus tard sous soixante jours à compter de la réception de la réclamation. L'entreprise dispose alors d'un délai de vingt-cinq jours pour s'y conformer. À défaut, le panel peut saisir la Commission Fédérale du Commerce américaine (*Federal Trade Commission* – FTC) en vue d'éventuelles sanctions, mais aussi informer toute autre organisation américaine, au niveau d'un État ou au niveau fédéral, comme par exemple le ministère du Commerce (DoC). Dans une telle hypothèse, le DoC peut ultimement choisir de retirer l'entreprise de la liste des organisations auto-certifiées au titre du *Privacy Shield* et de rendre public ce retrait.

En outre, la personne concernée peut toujours formuler sa plainte directement auprès de son autorité de protection des données personnelles nationale, laquelle transmettra la réclamation au DoC et/ou à la FTC. DoC comme FTC ont mis en place des points de contact et des procédures spécifiques en vue de faciliter le traitement des réclamations liées à l'application des principes du *Privacy Shield*. Seule la FTC peut être saisie directement par un citoyen européen.

Lorsque ni le contact direct de l'entreprise, ni les mécanismes de recours indépendants n'ont abouti à une réponse satisfaisante pour la personne concernée, un dernier recours est offert avec la possibilité de saisir le Comité d'arbitrage du *Privacy Shield* (*Privacy Shield Panel*). Ce Comité est composé d'au moins vingt arbitres choisis par le DoC et par la Commission européenne sur des critères d'indépendance, d'intégrité, et d'expérience en matière de protection des données en droit américain et droit européen. Un à trois arbitres officient lorsqu'une réclamation est portée devant le Comité. Les décisions sont rendues sous 90 jours et sont contraignantes pour les entreprises américaines auto-certifiées ; elles ont vocation à résoudre les litiges du point de vue des principes du *Privacy Shield* mais ne peuvent allouer de dommages et intérêts. Le Comité est établi aux États-Unis et fonctionne en langue anglaise ; cependant la personne concernée peut participer par téléphone ou visioconférence, obtenir gratuitement la traduction des documents mais également se faire assister par son autorité de protection des données personnelles nationale. En dehors des frais de représentation si les parties ont fait appel à des avocats pour les assister, toute la procédure est gratuite.

2. Différents organismes privés ont d'ores et déjà développé des programmes à ces fins, comme le Council of Better Business Bureau, TRUSTe, l'American Arbitration Association, JAMS, ou encore la Direct Marketing Association.

3. Les entreprises qui font ce choix (ou qui doivent se soumettre au contrôle du panel dans le cas du traitement de données RH) sont tenues de payer une redevance annuelle de 50 dollars afin de participer aux frais de fonctionnement du panel des DPA européennes.

En dehors des recours liés aux violations des principes de protection des données à caractère personnel, le *Privacy Shield* a également mis en place un mécanisme relatif aux données des citoyens européens transférées à des entreprises américaines[4], et qui auraient fait l'objet d'un accès par les agences gouvernementales américaines, pour des motifs de sécurité nationale. Est ainsi désigné un médiateur (*Ombudsperson*), haut fonctionnaire du Département d'État américain, qui peut être saisi par le biais de l'autorité de protection des données personnelles du pays de la personne concernée. Une demande formulée dans ce cadre n'a pas nécessairement à démontrer que des données ont effectivement fait l'objet de mesures de surveillance de la part d'une agence gouvernementale. Le Médiateur n'a pas vocation à confirmer ni infirmer l'existence d'un accès aux données mais, après enquête, certifiera le respect des lois et réglementations en vigueur aux États-Unis, encadrant de tels accès, ou bien précisera que des mesures correctives ont été prises, en cas de violation.

L'utilité de ce mécanisme peut être relativisée dès lors que le Médiateur n'a aucun pouvoir de contrainte sur les agences gouvernementales interrogées, ni ne peut divulguer de détails sur les mesures de surveillance ou les mesures correctives éventuellement appliquées. L'Ombudsperson est néanmoins un progrès pour les droits des Européens outre-Atlantique. Un guide pour les citoyens a été publié par la Commission européenne qui clarifie le processus de recours notamment[5].

d. La revue annuelle

Un examen conjoint annuel couvrira tous les aspects du fonctionnement de l'UE et des États-Unis à savoir la protection de la vie privée, y compris l'application des exceptions de la sécurité nationale et de l'application de la loi aux principes de protection de la vie privée. Pour effectuer un tel examen, la « *Commission de l'UE se réunira avec le Département du commerce et la FTC, accompagnée, le cas échéant, par d'autres ministères et organismes impliqués dans la mise en œuvre des arrangements relatifs au bouclier de protection de la vie privée* », les représentants du directeur du renseignement national (ODNI en anglais), d'autres éléments de la communauté du renseignement et l'Ombudsman. La participation à cette réunion sera ouverte aux autorités de protection des données de l'UE et aux représentants du groupe de travail « Article 29 » (considérant 122).

Cet examen comprendra des informations sur les plaintes reçues par le ministère du Commerce, des autorités de protection des données et sur les résultats des examens de conformité.

Un rapport public de la Commission européenne au Parlement européen et au Conseil sera rendu sur la base de l'examen annuel conjoint et d'autres sources d'information pertinentes (par exemple, rapports de transparence des entreprises).

La Commission organisera également un sommet annuel sur la protection de la vie privée avec les ONG et les parties intéressées afin de discuter des développements plus vastes dans le domaine du droit de la vie privée des États-Unis et de leur impact sur les Européens. En outre, la Commission, après l'adoption de cette décision, vérifiera périodiquement si la constatation relative à l'adéquation du niveau de protection garantie par les États-Unis d'Amérique est toujours effective. En tout état de cause, un tel contrôle est nécessaire lorsque la Commission acquiert des informations donnant lieu à un doute justifié à cet égard (considérant 120).

1.5. Les Traités d'assistance judiciaire mutuelle ou MLAT

Lors de son audition auprès de la Commission des affaires judiciaires de la Chambre des représentants des États-Unis, le directeur juridique de Microsoft a rappelé la nécessité de moderniser les Traités d'assistance judiciaire mutuelle entre les pays et a encouragé le Congrès et le Gouvernement à y travailler s'agissant de l'accès aux données de communications électroniques.

Certains traités existent déjà mais sont très peu utilisés au regard des lourdeurs de mise en œuvre. Il propose notamment (i) que nous passions de l'ère du papier au digital s'agissant des demandes d'information qui peuvent être faites et (ii) que les termes soient normalisés pour tous les pays afin de faciliter la revue des demandes, ce qui éviterait aux fournisseurs de service d'être confrontés à différents termes et obligations juridiques.

Ce travail requiert une coopération internationale des États qui peut mettre du temps car elle ne peut se faire sans le support des Gouvernements concernés. Par ailleurs, le nouvel arsenal juridique européen qu'est le Règlement général sur la protection des données personnelles dispose en son article 50 b) que « *la Commission et les autorités de contrôle prennent, à l'égard des pays tiers, les mesures appropriées pour : [...]*

b) se prêter mutuellement assistance sur le plan international dans l'application de la législation relative à la protection des données à caractère personnel, y compris par [...] l'entraide pour les enquêtes et les échanges d'informations, [...] ».

La Commission a donc aussi son rôle à jouer dans la mise en place de ces nouveaux cadres internationaux de coopération judiciaire avant mai 2018.

2. Le pouvoir législatif

Les limites du *Patriot Act*, de l'ECPA, du FISA énoncés ci-dessus ont conduit le Congrès à clarifier des dispositions du droit américain à travers plusieurs lois et propositions de lois en cours, afin de s'adapter à l'ère du digital et de rester cohérent avec les principes fondamentaux rappelés dans la Constitution américaine.

2.1. Le *Freedom Act*

Ce texte voté le 2 juin 2015 a pour vocation de modifier le *Patriot Act* et de mettre un terme à la collecte massive, automatique et indiscriminée des métadonnées téléphoniques des Américains. Jusque-là, les autorités avaient accès à toutes les don-

4. Ce mécanisme peut être mis en œuvre que les données aient été transférées aux Etats-Unis dans le cadre du *Privacy Shield* ou au moyen d'un autre cadre juridique : clauses contractuelles types, *Binding Corporate Rules* ou encore au titre d'une exception, actuelle ou future, au principe d'interdiction des transferts.

5. http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf?mkt_tok=eyJpIjoiTWpWbFlqQmpORGN3WldaaiIsInQiOiJIVmtvTGZXSUkzdXdYNVFGQkV2bodmaVlIVTBicDZZNExGMnZoRzBHUWtKOXdZM1JcL3NlS3pcL2hkbG5KYjNCSWooTHdtWEpJeUFxdGZWMzdjNkNRMkhzbG5pMnk2NDIxdEFZSFhkYVZjTDIwPSJ9.

nées téléphoniques des Américains via les opérateurs de téléphonie. Ce sont désormais les opérateurs téléphoniques qui seront chargés de conserver les métadonnées issues des conversations de la population américaine. Les compagnies de télécommunication fourniront ces informations au cas par cas, uniquement à la demande des services d'information.

Les autorités devront mettre en avant des « *critères spécifiques* » justifiant la demande de données. Parmi ces critères, il y a le lien avec le terrorisme, encore faut-il que ce lien soit « *raisonnable et circonstancié* ».

Le texte prévoit un renforcement du contrôle judiciaire sur l'exploitation des données.

Les autorités seront notamment tenues de dresser chaque année un rapport sur les activités de surveillance de la NSA, de supprimer les restrictions d'accès de certains rapports ou de résumer les opinions de la « *FISA Court* » les plus importantes.

Le gouvernement américain doit désormais communiquer au Congrès (et au public) chaque année le nombre de demandes et de directives de la FISA demandées et reçues, ainsi que des estimations du nombre de personnes américaines et non américaines visées par Surveillance. Cette loi a aussi permis aux fournisseurs de services informatiques d'être plus transparents sur ce sujet[6]. Microsoft affiche ainsi le nombre de demandes[7] faites par les autorités de police, et par les autorités de renseignements.

Cette loi a permis également de nommer cinq personnes, des juristes notamment, pour aider la FISA Court à se prononcer sur des interprétations nouvelles de la loi s'agissant de problématiques liées à la protection de la vie privée et des libertés civiles.

2.2. Le *Judicial Redress Act*

Cette loi signée par le Président Obama le 24 février 2016, clé de voûte dans l'approbation du *Privacy Shield* permet désormais aux citoyens non américains de se pourvoir en justice devant les juridictions américaines, si des agences gouvernementales américaines étaient amenées à violer des principes de protection de la vie privée tels qu'énoncés dans le *Privacy Act* de 1974[8].

Cette loi dispose que les Agences fédérales doivent notifier au public américain les dossiers électroniques sur les individus via le registre fédéral, interdit la divulgation d'un dossier sans son consentement écrit (avec des exceptions) et donne un droit d'accès et de modification aux Américains ou résidents américains.

« *En permettant aux citoyens européens et d'autres alliés américains désignés de bénéficier de procédures de protections de données semblables à celles qui sont proposées aux citoyens américains en Europe, les États-Unis peuvent fournir des droits égaux à nos partenaires commerciaux connexes en plus de promouvoir le progrès économique mondial* », a commenté Mark MacCarthy, vice-président senior de la politique publique de la SIIA (*Software & Information Industry Association*).

Ainsi, les recours ouverts aux citoyens américains en cas de violation du *Privacy Act*[9] de 1974 sont désormais ouverts aux Européens. Ces derniers peuvent également demander l'accès aux archives des agences fédérales au titre du *Freedom Of Information Act* (FOIA) de 1966, bien que diverses exceptions liées à la sécurité nationale empêchent l'accès aux informations classifiées.

Au moment où cet article est écrit, nous savons que le nouveau président des États-Unis, Donald Trump a signé deux décrets « anti-immigration ». Dans l'un d'entre eux, il est dit que les non-résidents permanents et les non-citoyens américains ne pourront bénéficier des dispositions du *Privacy Act* de 1974, (5 USC § 552 a), s'agissant de l'utilisation de leurs données personnelles par les agences fédérales.

Le *Privacy Act* n'a jamais prévu un champ d'application plus large que « *les citoyens des États-Unis ou un étranger légalement résident permanent* ». Pour autant, pour les fichiers mixtes qui contenaient des bases de données personnelles à la fois de citoyens américains et non américains, comme les dossiers d'immigration, d'Interpol du Département de la Justice et aux dossiers de réfugiés et visas rattachés au Département d'État, ou ceux des agences fédérales comme le Département de la sécurité intérieure (DHS), il était appliqué les mêmes règles de protection d'une manière indifférenciée[10].

Ce décret remet-il en cause le *Privacy Shield*, qui s'appuie sur un arsenal législatif américain, pour considérer que les États-Unis ont bien un système de protection adéquat à celui de l'UE ? Rien n'est moins sûr, car un décret pourrait-il remettre en cause une loi ? Néanmoins, le député européen Jan Philipp Albrecht craint que ce décret ne porte atteinte à l'accord garantissant la protection des données[11]. Toutefois, le *Privacy Shield* protège les données des citoyens de l'UE transférées aux États-Unis et non les données collectées aux États-Unis. La loi américaine sur la protection des renseignements personnels, le *Privacy Act*, ne couvre pas la protection des données des citoyens européens. En effet, Le *Privacy Shield* s'est appuyé, comme rappelé ci-dessus, sur le *Judicial Redress Act* notamment, et non le *Privacy Act*.

Toutefois, nous en saurons plus, lorsque la revue du *Privacy Shield* sera mené en juillet prochain par la Commission européenne pour évaluer l'efficacité et les modalités d'application pratiques du *Privacy Shield*. Comme rappelé par la porte-parole de la Commission : « *Nous continuerons à surveiller la mise en œuvre de ces deux instruments juridiques et nous suivons de près aux États-Unis tout changement qui pourrait avoir un impact sur les lois européennes relatives à la protection des données* »[12].

6. À titre d'exemple, le *Transparency Hub* de Microsoft : https://www.microsoft.com/about/csr/transparencyhub/fisa/
7. Les *electronic surveillance orders* (50 USC § 1805), FISA search warrants (50 USC § 1824), les « *FISA Amendments Act directives* » ou les demandes (50 USC § 1881 et seq.)
8. HR 1428 (114th) : *Judicial Redress Act* 2015-2016: https://www.govtrack.us/congress/bills/114/hr1428/summary
9. Le *Privacy Act* encadre la collecte, la conservation, l'utilisation et la diffusion des données personnelles des individus par les agences gouvernementales américaines. Il prévoit une publication des traitements sur un registre fédéral, prohibe la divulgation des données sans le consentement écrit de la personne (en dépit de certaines exceptions) et offre aux personnes un droit d'accès et de modification de leurs informations.
10. *DHS Privacy Office Policy Guidance Memorandum* 2007-1.
11. https://twitter.com/JanAlbrecht/status/824553926783907 84.
12. http://www.lemondeinformatique.fr/actualites/lire-selon-l-ue- le-decret-de-trump-ne-remet-pas-en-question-le-privacy-shield -67217.html.

Au surplus, aujourd'hui, quatre organisations – dont la Quadrature du Net, French Data Network et la Fédération FDN – considèrent que le *Privacy Shield* n'apporte pas un niveau suffisant de protection aux données personnelles des citoyens européens. Digital Rights a donc déposé un recours en annulation. L'issue de la procédure (affaire n° T-670/16) ne devrait pas être connue avant un an, voire plus.

2.3. L'*Email Privacy Act*[13]

Le projet de loi, initié en 2013 et enfin voté le 6 février 2016 a modifié l'ECPA (*Electronic Communications Privacy Act*) pour s'assurer que les autorités américaines obtiennent un mandat de perquisition avant de contraindre les entreprises de nouvelles technologies à divulguer du contenu de courriel et de toute communication électronique de leurs clients. Avant son entrée en vigueur, un vide juridique leur permettait d'obtenir des courriels par le biais d'une citation à comparaître et non d'un mandat. Cette loi est venue codifier également un jugement[14] qui a affirmé la nécessité d'obtenir un mandat en premier avant d'accéder à des courriels stockés dans un espace « *cloud* ».

2.4. L'*International Communications Privacy Act*[15]

Cette Proposition de loi déposée par plusieurs sénateurs dont Chris Coons (qui avait déjà, via le dépôt en 2014 puis 2015, proposé le *Law Enforcement Access to Data Stored Abroad Act*) en mai 2015, permettrait de conditionner la demande de divulgation de contenu de communications d'une autorité gouvernementale à des fournisseurs de services de communications électroniques ou de services de télécommunications à distance stockées en nuage dans un serveur situé hors des États-Unis, à un mandat de perquisition.

Le projet de loi permettrait à une entité gouvernementale d'obtenir ces communications seulement si un tribunal estime que l'entité gouvernementale a pris toutes les mesures raisonnables pour établir la nationalité et le lieu de l'abonné ou du client dont les communications sont demandées et qu'il y a des motifs raisonnables de croire que cet abonné ou le client est un Américain, un résident américain ou un ressortissant d'un pays étranger qui a conclu un accord de coopération avec les États-Unis en matière d'application de la loi.

Les lois sur la protection de la vie privée suivraient l'individu et donc seraient rattachées sa nationalité, plutôt qu'au lieu où ses données seraient stockées. Les Européens bénéficieraient de leur arsenal de protection sur leurs données personnelles quel que soit l'endroit où seraient stockées ses informations[16]. Cette idée a été retenue dans le cadre des négociations en cours entre les États-Unis et le Royaume-Uni.

Enfin, le ministère de la Justice contribuerait à améliorer les traités d'assistance mutuelle judiciaires avec les gouvernements étrangers.

3. Le pouvoir judiciaire

Les juges ne sont pas en reste sur la nécessité de réaffirmer des libertés civiles face à la toute-puissance des intérêts nationaux et impératifs de sécurité sans limite.

3.1. La *third party doctrine*

Pendant des années, la protection de la vie privée a été considérée comme dépassée. Marck Zuckenberg avait même dit « *the age of privacy is over* »[17]. Les juges avaient développé une doctrine selon laquelle le 4e amendement de la Constitution des États-Unis ne protège pas les données d'une personne si un tiers est déjà en sa possession. La théorie selon laquelle, à partir du moment où l'on confie ses données à un tiers, elles ne présentent plus un caractère privé s'est développée dans les années 1970 et 80 dans des cas où la Cour suprême devait se prononcer sur des fichiers de métadonnées téléphoniques liées à des affaires de fraude bancaires. Cette théorie permettait au Gouvernement de saisir des documents confiés aux entreprises par les particuliers sans mandat de perquisition ce qui aurait été obligatoire si la saisie était opérée au domicile de la personne concernée. En effet, le 4e amendement du *Bill of Rights* de 1789, protège les justiciables contre l'arbitraire judiciaire tel que l'interdiction des perquisitions et des saisies injustifiées, ce qui prenait tout son sens à l'ère du papier où les individus conservaient leurs informations sur des supports papiers et chez eux. Toutefois, à l'ère du digital où la majorité des individus utilise le digital pour échanger des informations d'ordre privé, il faut restaurer la force du 4e amendement. Les révélations d'Edward Snowden sur les programmes de surveillance des agences de renseignement américaines ont réveillé les consciences et les utilisateurs de nouvelles technologies exigent aujourd'hui de leurs fournisseurs des garanties de sécurité et de confidentialité.

3.2. L'affaire *Riley c/ California*[18]

Les décisions des tribunaux ont commencé à évoluer. Le 25 juin 2014, dans une affaire opposant M. Riley à l'État de Californie, a été déclaré inconstitutionnelle une perquisition sur le contenu d'un téléphone portable sans un mandat du juge. Cette affaire était une étape majeure pour faire respecter les dispositions du 4e amendement, étant entendu qu'aujourd'hui, nos vies privées sont très souvent stockées sur nos téléphones portables. Il faut donc désormais aux autorités de police un mandat de perquisition délivré par le juge pour pouvoir avoir accès à des données personnelles.

3.3. Le *Warrant case* de Microsoft

Dans ce contexte intrusif, certaines grandes entreprises du numérique ont souhaité remettre en cause les pratiques du gouvernement américain en matière de surveillance devant les juges afin d'influencer le mouvement de réformes actuel aux États-Unis en matière de protection de la vie privée et des données personnelles, avec

13. http://www.reuters.com/article/us-usa-congress-emails-idUSKBN15L2N3.
14. *États-Unis c/ Warshak*.
15. https://www.congress.gov/bill/114th-congress/senate-bill/2986?resultIndex=164.
16. https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case/.
17. https://www.youtube.com/watch?v=Tqu1O57AG_8.
18. https://epic.org/amicus/cell-phone/riley/riley-v-california.pdf.

notamment l'*International Communications Privacy Act*, projet de loi fédérale qui viendrait établir des règles claires en matière d'accès extraterritorial aux données et limiter les hypothèses dans lesquelles le gouvernement américain pourrait demander l'accès à des données stockées hors du territoire américain.

Parmi ces remises en cause, il est important de mentionner le Warrant Case, introduit par Microsoft en 2013. En l'espèce, le gouvernement américain avait demandé, dans le cadre d'une citation à comparaître (*subpoena*) prévue par l'ECPA, à Microsoft de lui donner accès aux données d'un client (des données de contenu comme des métadonnées concernant l'inscription et l'utilisation du compte du client) du service d'email gratuit et en ligne de Microsoft. Si les métadonnées étaient stockées sur le sol américain, et ont donc pu être transmises au gouvernement américain dans le cadre de cette citation à comparaître, il en allait autrement des données de contenu de ce client, stockées dans un *datacenter* irlandais de Microsoft. Pour ces dernières, Microsoft a refusé de donner l'accès au gouvernement américain. En effet, Microsoft a fait valoir que le contenu des courriels n'appartenait qu'à ses clients et n'était donc pas sous son contrôle[19]. Par ailleurs, le gouvernement américain avait pour obligation d'utiliser un mandat de perquisition plutôt qu'une citation à comparaître pour demander la communication du contenu des emails stockés en Irlande[20]. Le 14 juillet dernier, la cour d'appel du Second Circuit a donné raison à Microsoft, concluant que le gouvernement américain ne pouvait unilatéralement contraindre Microsoft à lui donner accès à des données stockées exclusivement en dehors des États-Unis et devait dès lors faire appel aux traités d'assistance judiciaire mutuelle et qu'un mandat de perquisition n'était pas suffisant[21]. Le Gouvernement avait fait appel par la procédure de « l'en banc » afin que l'arrêt soit revu, la cour d'appel a refusé le 24 janvier dernier cette demande et confirmé l'arrêt rendu[22].

3.4. L'encadrement des *secrecy orders*

Plus récemment, en avril 2016, Microsoft a de nouveau remis en cause la pratique du gouvernement américain selon laquelle ce dernier interdisait aux fournisseurs de service internet de notifier les clients concernés par des demandes d'accès à leurs données sous le régime de l'ECPA. En effet, Microsoft considère que ces restrictions vont à l'encontre même de ce que la Constitution américaine prévoit dans son quatrième amendement, consacré au droit des citoyens à savoir s'ils font l'objet d'une procédure de perquisition ou de recherches. Cette nécessaire transparence du Gouvernement que l'industrie des nouvelles technologies réclame, conditionne la confiance qu'auront les utilisateurs dans leurs outils où la donnée est transférée d'un endroit de la planète à un autre lorsqu'elle est dans le « *cloud* ».

3.5. Les organisations gardiennes des libertés civiles

En 2008, il est intéressant de voir que plusieurs organisations privées[23] après que John Ruggie, représentant spécial du Secrétaire général des Nations unies dans ses rapports de 2008 et 2011, ait proposé l'élaboration de principes pour une société plus responsable. Ainsi en 2008, des entreprises du secteur des technologies de l'information et de la communication (TIC), des investisseurs, des organisations de la société civile, des ONG, des universitaires se sont réunis pour dresser des principes et directives qui forment un cadre global qui « *entend guider et conseiller le secteur des TIC et ses parties prenantes en vue d'assurer à l'échelle de la planète la protection et la promotion de la jouissance des droits de l'homme* », dont le respect de la vie privée.

La possibilité pour des tiers de se joindre à la cause d'une action judiciaire introduite par une personne, qu'on appelle Amicus Brief a permis à la société civile de se joindre à la cause de Microsoft dans son combat contre le Gouvernement américain susvisé. C'est ainsi que Verizon, l'Electronic Frontier Foundation, Apple, Cisco, l'État irlandais, le parlementaire Jan Philipp Albrecht ont pu se rallier à la cause.

La résultante de ce combat sur le transfert des données et leurs accès par les Gouvernements se résume en quatre points. Les gouvernements (i) devraient avoir accès sur le propre territoire à des données personnelles uniquement conformément aux moyens légaux, (ii) ne doivent pas pouvoir exiger d'avoir accès au-delà de leurs frontières géographiques à des contenus de courriels ou tout autre contenu privé de citoyens étrangers sans passer par des traités d'assistance judiciaire mutuelle, (iii) ne doivent pouvoir exiger d'avoir accès, qu'en application de leurs dispositifs légaux, à des données en dehors de leur territoire que pour celles appartenant à leurs ressortissants et (iv) doivent respecter les lois sur la protection de la vie privé des autres pays.

Si le débat continue sur le *Privacy Shield*, un autre s'ouvre sur les clauses contractuelles types, puisque les récentes déclarations de l'autorité de protection des données personnelles irlandaise (IDPC) a déclaré le 25 mai dernier, par la voix d'Helen Dixon, son commissaire à la protection des données, avoir des doutes sur leur conformité aux réglementations européennes. Elle a donc demandé à la CJUE de se prononcer sur le statut juridique des transferts de données effectués sous le régime des clauses contractuelles types.

Gageons que la décision de la CJUE prendra un certain temps et que nos Gouvernements trouveront entretemps la solution qui permettra de préserver les centaines de milliers de transactions entre l'UE et les autres pays. ■

19. Voir, au contraire, *United States c/ Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984); *Marc Rich & Co., A.G. c/ United States*, 707 F.2d 663 (2nd Cir.1983).
20. Voir *United States c/Warshak*, 631 F.3d 266 (6th Cir. 2010).
21. *Microsoft c/ United States*, No. 14-2985, 2016 BL 225943 (2d Cir. July 14, 2016) (15 PVLR 1465, 7/18/16) ; voir aussi *United States c/ Bin Laden*, 126 F. Supp. 2d 264 (SDNY 2000).
22. http://actonline.org/2017/01/25/highly-impactful-u-s-federal-court-decision-on-law-enforcement-access-to-data-stored-abroad-status-next-steps-and-other-moving-pieces/.
23. https://www.globalnetworkinitiative.org/sites/default/files/pdfs/FR_Principles_FRA.pdf.