COMMISSION
EUROPÉENNE

Bruxelles, le 29.2.2016
COM(2016) 117 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides

1. INTRODUCTION : LE ROLE DES ECHANGES DE DONNEES A CARACTERE PERSONNEL DANS LES RELATIONS UE-ÉTATS-UNIS

Un solide partenariat transatlantique entre l'Union européenne et les États-Unis est aujourd'hui plus vital que jamais. Nous partageons des valeurs communes, nous poursuivons des objectifs politiques et économiques communs, et nous coopérons étroitement dans la lutte contre les menaces communes pour notre sécurité. L'ampleur de nos échanges commerciaux et notre coopération étroite dans les affaires internationales témoignent de la force durable de notre relation.

Le transfert et l'échange de données à caractère personnel sont un aspect essentiel sur lequel reposent les liens étroits que l'Union européenne (UE) et les États-Unis entretiennent dans le secteur commercial ainsi que dans le domaine des services répressifs. Ces échanges de données requièrent un haut niveau de protection des données et l'adoption de garanties adéquates.

En juin 2013, des révélations concernant l'existence de programmes de collecte massive de renseignements aux États-Unis ont suscité de sérieuses inquiétudes, tant au niveau de l'UE que de ses États membres, quant aux conséquences que ces traitements de données à caractère personnel réalisés à grande échelle par les autorités publiques et les entreprises privées aux États-Unis pourraient avoir sur les droits fondamentaux des Européens.

En réaction à ces révélations, le 27 novembre 2013, la Commission a publié une communication visant à rétablir la confiance dans les flux de données entre l'UE et les États Unis[1], qui présentait un plan d'action pour redonner confiance dans les transferts de données, dans l'intérêt de l'économie numérique, de la protection des droits des citoyens européens et des relations transatlantiques au sens plus large. Pour atteindre cet objectif, la communication prévoyait les mesures clés suivantes:

(i) adopter le train de réformes sur la protection des données proposé par la Commission en 2012[2];

(ii) rendre la sphère de sécurité plus sûre, sur la base des 13 recommandations énoncées dans la communication sur la sphère de sécurité[3]; et

---

[1] Communication de la Commission au Parlement européen et au Conseil intitulée «Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique», COM(2013) 846 final, 27.11.2013 (ci-après dénommée «la communication de 2013» ou «la communication»), disponible sur : http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[2] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final du 25.1.2012, et 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), COM(2012) 11 final du 25.1.2012, disponible sur : http://ec.europa.eu/justice/data-protection/reform/index_fr.htm

(iii) renforcer les garanties en matière de protection des données pour la coopération entre les services répressifs, notamment par la conclusion des négociations sur l'accord-cadre sur la protection des données entre l'UE et les États-Unis. Ce dernier énonçait également l'objectif d'obtenir des engagements de la part des États-Unis concernant des droits individuels opposables, notamment la possibilité d'exercer des recours juridictionnels, en particulier après l'adoption de la «Judicial Redress Act» (loi sur le recours juridictionnel) étendant aux citoyens de l'UE certains droits inscrits dans la loi de 1974 sur la protection de la vie privée (ci-après, «Privacy Act») qui, à l'époque, ne pouvaient être invoqués que par les citoyens et résidents permanents aux États-Unis.

Ces objectifs ont été réaffirmés dans les orientations politiques[4] de la Commission Juncker : «*La protection des données est un droit fondamental revêtant une importance particulière à l'ère numérique. En plus de finaliser rapidement les travaux législatifs sur les règles communes de l'Union en matière de protection des données, nous devons aussi faire reconnaître ce droit dans le cadre de nos relations extérieures. À la suite des révélations récentes concernant une surveillance de masse, nos partenaires proches que sont les États-Unis vont devoir nous convaincre que les arrangements concernant la "sphère de sécurité" sont réellement sûrs, s'ils veulent qu'ils soient maintenus. Les États-Unis doivent également garantir que tous les citoyens de l'UE, qu'ils résident ou non aux États-Unis, ont le droit de faire valoir leurs droits à la protection des données devant les tribunaux américains. Ce point sera essentiel pour rétablir la confiance dans les relations transatlantiques.*»

Depuis lors, la Commission a travaillé en ce sens. Elle a accéléré les négociations sur l'accord-cadre, qui a été paraphé par les parties le 8 septembre 2015. Les discussions interinstitutionnelles sur le train de réformes de la protection des données se sont intensifiées, aboutissant à un accord politique entre le Conseil et le Parlement européen le 15 décembre 2015. En ce qui concerne les transferts transatlantiques de données dans le domaine commercial, la Commission a entamé des discussions avec les États-Unis pour renforcer la sphère de sécurité, en janvier 2014. L'invalidation de la décision sur la sphère de sécurité par la Cour de justice, dans l'arrêt *Schrems* du 6 octobre 2015[5], a confirmé la nécessité de disposer d'un nouveau cadre et a donné des indications sur les conditions que ce dernier devrait remplir. À la suite de cette décision, le 6 novembre 2015, la Commission a publié des orientations pour les entreprises, qui présentaient des outils alternatifs permettant de poursuivre les transferts de données à caractère personnel vers les États-Unis[6]. Le 2 février

---

[3] Communication de la Commission au Parlement européen et du Conseil sur le fonctionnement de la sphère de sécurité du point de vue des citoyens de l'UE et des entreprises établies sur son territoire, COM(2013) 847 final du 27.11.2013, pp. 18-19 (ci-après dénommée «la communication sur la sphère de sécurité»), disponible sur : http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

[4] Un nouvel élan pour l'Europe : Mon programme pour l'emploi, la croissance, l'équité et le changement démocratique - Orientations politiques pour la prochaine Commission européenne.

[5] Arrêt du 6 octobre 2015 dans l'affaire C-362/14, Maximilian Schrems/Data Protection Commissioner, EU:C:2015:650.

[6] Consulter la communication de la Commission au Parlement européen et au Conseil concernant le transfert transatlantique de données à caractère personnel conformément à la directive 95/46/CE faisant suite à l'arrêt de la Cour de justice dans l'affaire C-362/14 (Schrems), COM(2015) 566 final, 6.11.2015. Consulter également la déclaration du groupe de travail «Article 29» sur les conséquences de l'arrêt *Schrems* du 3 février 2016,

2016, un accord politique a été conclu au sujet d'un nouveau cadre pour les flux transatlantiques de données, le «bouclier vie privée UE-États-Unis»[7], en remplacement de l'accord précédent.

Ces résultats seront bénéfiques aux relations transatlantiques et devraient redonner aux Européens confiance dans l'économie numérique tout en renforçant leurs droits fondamentaux. Elles doteront également l'UE et ses États membres d'un cadre juridique plus solide pour la protection des données, qui conduira à une plus grande intégration du marché intérieur, en particulier le marché unique numérique, et permettra à l'UE d'intensifier ses efforts pour promouvoir et développer des normes internationales de protection de la vie privée et des données à caractère personnel.

Des initiatives importantes ont vu le jour par ailleurs, qui ont conduit à des changements significatifs dans l'ordre juridique des États-Unis. Le 17 janvier 2014, le président Obama a annoncé[8] des réformes concernant les activités de renseignements d'origine électromagnétique, qui ont ensuite été inscrites dans la directive présidentielle n° 28 (PPD-28)[9]. Fait important, ces réformes prévoyaient d'étendre certaines mesures de protection de la vie privée aux personnes n'ayant pas la nationalité américaine et de recentrer la collecte de données, jusque-là massive, pour privilégier une collecte et un accès ciblés. La Commission a accueilli favorablement ces nouvelles orientations, estimant qu'elles constituaient un pas important dans la bonne direction[10]. Ce processus de réforme a également contribué à alimenter les discussions avec les États-Unis sur le «bouclier vie privée UE-États-Unis». Depuis lors, d'autres modifications ont été apportées. Par exemple, en juin 2015, les États-Unis ont adopté la loi sur la sécurité intérieure, la «Freedom Act»[11], qui a modifié certains programmes de surveillance américains, renforcé le contrôle par le pouvoir judiciaire et accru la transparence publique quant à leur utilisation. Enfin, le 10 février 2016, le Congrès américain a adopté la «Judicial Redress Act» (loi sur le recours juridictionnel), promulgué par le président Obama le 24 février 2016[12].

C'est dans ce contexte que la présente communication fait le point, pour savoir jusqu'à quel point nous avons réalisé les objectifs formulés dans la communication 2013. Elle mettra également en évidence les domaines dans lesquels des efforts supplémentaires sont nécessaires pour consolider et rétablir totalement la confiance dans les flux transatlantiques de données.

---

disponible sur : http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[7] Voir http://europa.eu/rapid/press-release_IP-16-216_fr.htm

[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence

[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm

[11] USA FREEDOM Act of 2015, Pub. L., No. 114-23, § 401, 129 Stat. 268.

[12] H.R.1428 - Judicial Redress Act of 2015. Elle entrera en vigueur 90 jours après son adoption.

2. LA REFORME DE LA PROTECTION DES DONNEES DANS L'UE

2.1 Le contexte

Afin de saisir les opportunités offertes par un monde numérique de plus en plus interconnecté et de relever les défis qu'il pose, la Commission européenne a présenté son train de réformes sur la protection des données («la réforme») en janvier 2012. En renforçant les règles internes de l'UE et en permettant aux individus de mieux contrôler les données à caractère personnel qui les concernent, la réforme vise à accroître la confiance dans l'économie numérique, que ces données soient traitées dans un seul État membre, dans l'UE ou dans des pays tiers tels que les États-Unis.

Le train de réformes comprend deux instruments juridiques, un règlement général sur la protection des données[13] («le règlement»), qui établit un cadre européen commun pour la protection des données, et une directive sur la protection des données dans le domaine de la coopération policière et judiciaire («la directive sur la police»)[14]. En proposant un règlement qui sera directement applicable dans les États membres, la Commission entendait établir une norme commune de protection des données pour tous, qui éliminerait ainsi les niveaux de protection divergents entre les États membres. De même, la directive sur la police établira, pour la toute première fois, un corps commun de règles au niveau de l'UE, tout en tenant compte des spécificités des traditions judiciaires et policières des États membres.

Le 15 décembre 2015, le Parlement européen et le Conseil sont arrivés à un accord politique sur le train de réformes et ont ainsi mené à bien une des actions clés énoncées dans la communication de 2013.

2.2 Qu'est-ce qui a changé ?

Le règlement actualise, modernise et, dans certains cas, renforce les principes de la protection des données énoncés dans la directive sur la protection des données de 1995[15] pour garantir le droit à la vie privée. Il est axé sur le renforcement des droits des personnes, l'approfondissement du marché intérieur européen, un contrôle plus strict du respect des règles, la rationalisation des transferts internationaux de données à caractère personnel et l'établissement de normes globales de protection de données. Les règles sont conçues pour garantir la protection des données à caractère personnel des citoyens européens – quel que soit le lieu où celles-ci sont envoyées, traitées ou stockées – même en dehors de l'UE, comme c'est souvent le cas dans le monde numérique. Il est particulièrement utile de souligner certaines caractéristiques de la réforme.

Premièrement, le **champ d'application territorial :** le règlement indique clairement qu'il s'applique également aux sociétés établies dans un pays tiers si elles offrent des biens et services, ou observent le comportement des personnes, dans l'Union européenne. Les entreprises basées à l'extérieur de l'UE devront appliquer les mêmes règles que les entreprises

[13] COM(2012) 11 final du 25.1.2012: voir la note 2
[14] COM(2012) 10 final du 25.1.2012: voir la note 2
[15] 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, JO L 281 du 23.11.95, p. 31 («directive sur la protection des données»).

basées au sein de l'UE, de sorte à garantir une protection complète des droits des citoyens européens. Cela met également les entreprises européennes et étrangères sur un pied d'égalité, évitant ainsi des écarts de compétitivité lorsque les entreprises étrangères exercent des activités dans l'UE ou ciblent les consommateurs sur son territoire.

Deuxièmement, **un contrôle plus strict de** l'**application** des règles de protection des données : le règlement prévoit un régime de sanctions efficace en harmonisant les pouvoirs des autorités nationales chargées de la protection des données (DPA). Ces dernières seront habilitées à imposer des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise. Ce pouvoir d'imposer des sanctions dissuasives en cas de non-respect des règles de protection des données, conjugué avec le champ d'application territorial mentionné ci-dessus, fera en sorte que les entreprises exerçant des activités dans l'UE auront tout intérêt à se conformer à la législation de l'UE. Les nouvelles règles introduisent également un régime de responsabilité plus clair et plus sévère pour les sous-traitants et les responsables du traitement.

Troisièmement, **des règles harmonisées pour la coopération des services répressifs :** la directive sur la police appliquera les règles et principes généraux de la protection des données aux traitements de données à caractère personnel effectués par les autorités policières et judiciaires dans les États membres en matière de répression pénale. Il s'agit notamment de règles harmonisées pour les transferts internationaux de données à caractère personnel dans le cadre de la coopération en matière de répression pénale[16]. La nouvelle directive élèvera le niveau de protection des personnes physiques et garantira que les données relatives aux victimes, aux témoins et aux suspects sont dûment protégées dans le cadre des enquêtes criminelles ou des actions répressives. Le contrôle est assuré par les autorités nationales indépendantes de protection des données et les personnes doivent bénéficier de recours judiciaires effectifs. En parallèle, des lois plus harmonisées permettront à la police et aux autorités judiciaires de coopérer plus efficacement, entre États membres ainsi qu'entre ces derniers et leurs partenaires internationaux, pour lutter plus efficacement contre la criminalité et le terrorisme. Il s'agit là d'un volet crucial du programme européen en matière de sécurité[17].

Quatrièmement, **des règles strictes pour des transferts internationaux plus sûrs :** le règlement et la directive sur la police définissent des règles transparentes, détaillées et complètes pour les transferts de données à caractère personnel vers des pays tiers. Elles couvrent toutes les formes de transferts internationaux, qu'ils soient effectués à des fins commerciales ou pénales, entre des personnes privées ou des pouvoirs publics, ou entre autorités publiques et entreprises privées. Si la structure des règles sur les transferts internationaux reste essentiellement la même que dans l'actuelle directive sur la protection

[16] Contrairement à la décision-cadre du Conseil 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, qui ne couvre que les échanges transfrontaliers de données entre les autorités compétentes des États membres, l'application de ces règles en vertu de la directive sur la police ne dépendra plus de savoir si ces données ont préalablement été échangées entre les autorités pénales des États membres.

[17] Voir la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions — Le programme européen en matière de sécurité, COM(2015) 185 final du 28.4.2015.

des données (décisions constatant un niveau de protection adéquat, clauses contractuelles types et règles d'entreprise contraignantes, ainsi que certaines dérogations à l'interdiction générale de transférer des données à caractère personnel hors de l'UE), la réforme clarifie et simplifie ces règles de plusieurs manières tout en réduisant les formalités administratives. Elle ajoute également quelques nouveaux outils pour les transferts internationaux.

Le règlement renforce en outre les **pouvoirs des autorités de l'UE chargées de la protection des données**, notamment en ce qui concerne les transferts internationaux. Par rapport à l'actuelle directive sur la protection des données, les dispositions relatives à l'indépendance, aux fonctions et aux pouvoirs de ces autorités sont davantage détaillées et considérablement accrues. Cela inclut expressément le pouvoir de suspendre les flux de données vers un destinataire se trouvant dans un pays tiers ou à une organisation internationale. La directive sur la police contient des dispositions similaires en ce qui concerne les transferts internationaux et les pouvoirs des autorités de protection des données à l'égard du secteur répressif.

Plus précisément, en ce qui concerne les règles relatives aux décisions de la Commission constatant un niveau de protection **adéquat**, le règlement prévoit un catalogue détaillé et précis des éléments dont la Commission doit tenir compte lorsqu'elle évalue le niveau de protection des données prévu dans l'ordre juridique d'un pays tiers. Ce processus consiste en une évaluation globale que la Commission doit entreprendre et qui devrait couvrir – un élément qui est également conforme à l'arrêt *Schrems* – les règles régissant l'accès des autorités publiques d'un pays tiers aux données à caractère personnel. Une autre caractéristique essentielle de cette évaluation est que les personnes physiques jouissent d'un droit à la protection des données effectif et opposable et disposent de voies de recours administratives et judiciaires effectives.

De plus, le règlement exige expressément que la Commission **réexamine périodiquement**, au moins tous les quatre ans, toutes ses décisions constatant un niveau de protection adéquat, afin de rester en prise avec toutes les évolutions survenant dans un pays tiers qui pourraient avoir un impact direct, voire négatif, sur le niveau de protection dans son ordre juridique. Cette surveillance continue du niveau de protection adéquat sera un processus plus dynamique, car il impliquera également un dialogue avec les autorités du pays tiers en question.

En ce qui concerne les transferts vers des pays tiers pour lesquels il n'y a aucune décision constatant un niveau de protection adéquat, le règlement prévoit les conditions d'utilisation des **autres outils de transfert,** tels que les clauses contractuelles types et les règles d'entreprise contraignantes. Il ajoute également d'autres instruments pour les transferts, comme les codes de conduite agréés et les mécanismes de certification approuvés. Enfin, il clarifie la situation lorsque **des dérogations** sont autorisées.

2.3 La voie à suivre

La réforme de la protection des données constitue une étape essentielle pour renforcer les droits fondamentaux des citoyens à l'ère du numérique et pour faciliter les échanges commerciaux en simplifiant les règles applicables aux entreprises sur le marché unique

numérique. La confiance des consommateurs dans l'Union européenne et dans les opérateurs des pays tiers stimulera l'économie numérique européenne et mondiale et lui sera donc bénéfique. Elle aura des retombées positives sur nos relations commerciales avec les États-Unis, notre premier partenaire commercial. Elle clarifiera la situation et assurera un environnement stable à l'UE et aux entreprises étrangères. De leur côté, les entreprises américaines bénéficieront de la sécurité juridique qu'apporte un espace économique intégré qui applique un ensemble uniforme de règles sur la protection des données.

Les règles communes applicables au secteur répressif garantiront aux personnes physiques une meilleure protection des données les concernant et un droit de recours effectif. En facilitant la coopération transfrontière entre les autorités policières et judiciaires des États membres, on augmentera l'efficacité des services répressifs et on créera ainsi les conditions nécessaires à une prévention plus efficace de la criminalité dans l'Union européenne. En même temps, cela permettra une coopération plus aisée avec leurs homologues des pays tiers.

L'adoption formelle du train de réformes par le Parlement européen et le Conseil devrait avoir lieu au cours du premier semestre 2016. Le règlement s'appliquera deux ans après son adoption, tandis que la directive sur la police prévoit une période de mise en œuvre de deux ans. Toutes les parties prenantes concernées, à l'intérieur et à l'extérieur de l'UE, devraient mettre la période de transition de deux ans à profit pour se préparer aux nouvelles règles. La Commission jouera son rôle. Au cours de cette période de transition, elle travaillera en étroite collaboration avec les États membres, les autorités chargées de la protection des données et les autres parties intéressées pour assurer une application uniforme des règles et promouvoir un environnement propice à leur respect.

3. LE «BOUCLIER VIE PRIVEE UE-ÉTATS-UNIS» : UN NOUVEAU CADRE TRANSATLANTIQUE POUR LES FLUX DE DONNEES A CARACTERE PERSONNEL

3.1 Le contexte

Afin de faciliter les flux de données à caractère personnel entre l'UE et les États-Unis, destinés aux échanges commerciaux, tout en assurant la protection de ces données, la Commission avait, en 2000, reconnu que le cadre de la «sphère de sécurité» assurait un niveau de protection adéquat[18]. Ainsi, malgré l'absence d'une législation générale sur la protection des données aux États-Unis, les données à caractère personnel pouvaient être librement transférées à partir des États membres vers les entreprises aux États-Unis qui avaient souscrit aux principes de confidentialité qui sous-tendaient le cadre.

[18] Décision 2000/520/CE de la Commission du 20 juillet 2000. Dans cette décision, fondée sur l'article 25, paragraphe 6, de la directive sur la protection des données, la Commission avait reconnu que les principes de la «sphère de sécurité» et les questions fréquemment posées y afférentes, publiées par le ministère du commerce des États-Unis, offraient un niveau de protection adéquat aux fins du transfert de données à caractère personnel depuis l'UE. Le fonctionnement de l'accord sur la «sphère de sécurité» reposait sur les engagements et l'autocertification des entreprises qui y avaient adhéré. Les règles étaient contraignantes en droit américain pour ces entités et leur exécution pouvait être imposée par la U.S. Federal Trade Commission.

Dans sa communication de 2013 relative à la «sphère de sécurité»[19], la Commission a relevé un certain nombre de faiblesses dans le fonctionnement de l'accord au fil du temps, notamment un manque de transparence des entreprises concernant leur souscription au régime et une absence d'intervention des autorités américaines pour faire respecter les principes du régime par ces sociétés. Par ailleurs, les révélations faisant état d'une surveillance, publiées plus tôt dans l'année, avaient suscité des inquiétudes quant à l'ampleur et à la portée de certains programmes de renseignements américains et au degré d'accès par les autorités publiques américaines aux données à caractère personnel des Européens, transférées dans le cadre de la «sphère de sécurité». En considération de ces éléments ainsi que d'autres[20], la Commission a conclu que la «sphère de sécurité» devait être revue. Dans ce contexte, elle a formulé 13 recommandations[21] visant à renforcer et à actualiser les garanties en matière de protection des données intégrées dans ce cadre. Ces recommandations portaient sur : (i) le renforcement des principes de fond protégeant la vie privée et une plus grande transparence des politiques de confidentialité des entreprises américaines autocertifiées incorporant ces principes ; (ii) un contrôle, un suivi et une mise en œuvre améliorés et effectifs, par les autorités américaines, du respect des principes par les sociétés ; (iii) la mise en place de mécanismes de règlement des litiges abordables pour les plaintes des particuliers; et (iv) la nécessité que le recours à la dérogation pour raison de sécurité nationale ou de respect de la loi, prévue dans la décision de 2000 sur la sphère de sécurité, soit limité à ce qui est strictement nécessaire et proportionné.

Sur la base de ces 13 recommandations, la Commission a engagé des discussions avec les autorités américaines en janvier 2014. L'invalidation ultérieure de la décision sur la sphère de sécurité, le 6 octobre 2015, par la Cour de justice a confirmé la nécessité d'adopter un nouveau cadre plus solide pour les flux transatlantiques de données commerciales. Si la décision de la Cour s'appuie sur les recommandations de la Commission de 2013, elle souligne en outre la nécessité d'instaurer des limites, des garanties et des mécanismes de contrôle juridictionnel afin d'assurer la protection continue des données à caractère personnel des citoyens européens, y compris lorsque les données sont accessibles et utilisées par les pouvoirs publics aux fins de la sécurité nationale, de l'intérêt public ou du respect des lois.

Le 2 février 2016, après deux années d'intenses discussions, l'UE et les États-Unis ont abouti à un accord politique sur le nouveau cadre, le «bouclier vie privée UE-États-Unis». Ce nouvel accord comprend d'importantes garanties nouvelles et garantira un niveau élevé de protection des droits fondamentaux des citoyens européens. Il offrira la sécurité juridique nécessaire aux entreprises des deux côtés de l'Atlantique qui veulent faire des affaires ensemble et donnera un nouvel élan au partenariat transatlantique.

À l'issue des négociations avec les États-Unis, la Commission présentera le nouvel accord au groupe de travail «Article 29» (comprenant les autorités de protection des données de l'UE)

[19] Voir la note de bas de page 3.

[20] Ces éléments incluaient l'augmentation exponentielle des flux de données et leur importance cruciale pour l'économie transatlantique, ainsi que la rapide croissance du nombre de sociétés américaines souscrivant au régime de la sphère de sécurité. Voir la communication sur la sphère de sécurité, p. 37.

[21] Communication sur la sphère de sécurité, pp. 18-19.

pour obtenir un avis sur le niveau de protection offert. En outre, la décision constatant un niveau de protection adéquat passera par la procédure de comitologie avant d'être adoptée. Le contrôleur européen de la protection des données sera lui aussi consulté.

3.2 Qu'est-ce qui a changé ?

Le «bouclier vie privée UE-États-Unis» donne une suite solide et efficace aux 13 recommandations de la Commission et à l'arrêt *Schrems*. Il comporte un certain nombre d'améliorations substantielles, par rapport au cadre précédent, en ce qui concerne les engagements qui doivent être pris par les sociétés américaines. Il contient également de nouveaux engagements importants et des explications détaillées sur la législation pertinente des États-Unis et les pratiques des autorités américaines. Contrairement au texte précédent, le «bouclier vie privée» recouvre non seulement des engagements dans le secteur commercial mais aussi, et c'est une première importante dans les relations UE-États-Unis, en matière d'accès aux données à caractère personnel par les autorités publiques, y compris à des fins de sécurité nationale. C'est là un aspect essentiel et nécessaire, à la lumière de la jurisprudence de la Cour, pour rétablir la confiance dans les relations transatlantiques après les révélations au sujet de la surveillance exercée.

Les aspects positifs les plus importants de ce nouvel accord peuvent être regroupés en quatre catégories principales :

Premièrement, des **obligations strictes imposées aux entreprises et une application rigoureuse :** le nouvel accord sera plus transparent et comportera des mécanismes de contrôle efficaces pour que les entreprises suivent les règles qu'elles se sont juridiquement engagées à respecter. Les entreprises américaines qui souhaitent importer des données à caractère personnel à partir de l'Europe, au titre du «bouclier vie privée», devront accepter les obligations régissant le traitement de ces données et garantissant les droits des personnes. Cela inclut des conditions restreintes et des dispositions plus sévères en matière de responsabilité pour les entreprises souscrivant au «bouclier vie privée» qui transfèrent des données de l'UE, par exemple pour des activités de sous-traitance, à des tiers qui sont en dehors du cadre, que ce soit aux États-Unis ou dans d'autres pays tiers («transferts ultérieurs»). En ce qui concerne le contrôle, le ministère du commerce des États-Unis s'est engagé à effectuer un suivi régulier et rigoureux de la manière dont les entreprises se conforment à leurs engagements et à éliminer les «resquilleurs», c'est-à-dire les entreprises qui prétendent faussement adhérer au régime. Les engagements des entreprises sont juridiquement contraignants et exécutoires en vertu de la loi américaine par la Federal Trade Commission; les entreprises qui ne s'y conforment pas s'exposeront à des sanctions sévères.

Deuxièmement, **des limites et garanties précises concernant l'accès par le gouvernement américain:** pour la première fois, le gouvernement américain, par l'intermédiaire du ministère de la Justice et le Bureau du directeur des renseignements nationaux, en tant qu'organisme de supervision de tout le secteur du renseignement aux États-Unis, a fourni à l'UE des garanties écrites indiquant que l'accès des autorités publiques à des fins répressives, de sécurité nationale ou pour un autre intérêt public sera soumis à des limites et garanties précises et des dispositifs de contrôle. Les États-Unis créeront également un nouveau mécanisme de recours

destiné aux personnes concernées de l'UE, en matière de sécurité nationale, à savoir un médiateur qui sera indépendant des autorités nationales de sécurité. Ce médiateur sera chargé de répondre aux plaintes et aux demandes des citoyens européens à propos de l'accès pour raison de sécurité nationale et il devra confirmer à la personne que les lois pertinentes ont été respectées ou qu'il a été remédié à tout manquement. Il s'agit d'une évolution décisive qui s'appliquera non seulement aux transferts dans le cadre du «bouclier vie privée», mais aussi à *toutes les* données à caractère personnel transférées aux États-Unis à des fins commerciales, quelle que soit la raison invoquée pour transférer ces données.

Troisièmement, **une protection efficace du droit à la vie privée des citoyens européens, avec plusieurs possibilités de recours** : toute personne en Europe qui considère que les données la concernant ont fait l'objet d'une utilisation abusive dans le cadre du nouvel accord bénéficiera de plusieurs moyens de recours individuels accessibles et abordables, y compris des organismes de règlement extrajudiciaire des litiges gratuit. Les entreprises s'engagent à répondre aux plaintes dans un délai déterminé. En outre, toute entreprise manipulant des données en matière de ressources humaines provenant d'Europe doit s'engager à respecter les décisions des autorités compétentes de protection des données de l'UE, tandis que d'autres entreprises peuvent volontairement prendre un tel engagement. Les personnes physiques peuvent également déposer plainte auprès de «leur» autorité de protection des données, qui disposera d'une procédure formalisée pour transmettre les plaintes au ministère du commerce des États-Unis et à la Federal Trade Commission pour faciliter l'enquête et le règlement de la plainte dans un délai raisonnable. Néanmoins, si un cas n'est pas résolu par l'une de ces voies, les personnes seront en mesure de recourir, en dernier ressort, au Privacy Shield Panel, un mécanisme de règlement des litiges qui peut prendre des décisions contraignantes et exécutoires contre les entreprises américaines adhérant au «bouclier vie privée». En outre, les autorités de protection des données de l'UE pourront fournir une assistance aux personnes pour préparer leur dossier. Ainsi qu'il est mentionné ci-dessus, pour les plaintes concernant un éventuel accès par les services de renseignement nationaux, un nouveau médiateur sera institué, offrant ainsi une voie de recours supplémentaire.

Quatrièmement, un **mécanisme de réexamen conjoint annuel :** cela permettra à la Commission de contrôler régulièrement le fonctionnement de tous les aspects du «bouclier vie privée», y compris les limites et garanties relatives à l'accès pour raison de sécurité nationale. La Commission et le ministère américain du commerce procéderont au réexamen et y associeront les autorités de protection des données de l'UE, les autorités de la sécurité nationale américaine et le médiateur. De cette façon, les États-Unis seront tenus responsables de leurs engagements. Mais la Commission ne s'arrêtera pas là : elle s'appuiera également sur toutes les autres sources d'information disponibles, y compris les rapports de transparence volontaires établis par les entreprises sur le nombre de demandes d'accès par le gouvernement[22]. L'examen annuel va au-delà du nouveau règlement, qui impose de tels

[22] Les grandes sociétés internet américaines produisent déjà de tels rapports afin de regagner la confiance de leurs clients. La loi américaine FREEDOM Act de 2015 permet la publication de rapports volontaires sur les demandes d'accès, du moins dans certaines limites, afin de protéger les intérêts de la sécurité nationale.

réexamens seulement tous les quatre ans, ce qui démontre la volonté de l'UE et des États-Unis de faire respecter rigoureusement les règles.

Ce réexamen ne sera pas un exercice formaliste sans conséquence. Dans les cas où les entreprises ou les autorités publiques américaines ne respecteraient pas leurs engagements, la Commission activera le processus de suspension du «bouclier vie privée». Comme l'a souligné la Cour dans l'arrêt *Schrems*, une décision constatant un niveau de protection adéquat ne doit pas être lettre morte; au contraire, les autorités et les entreprises américaines doivent insuffler vie au cadre et l'alimenter en permanence en honorant leurs engagements. À défaut, l'avantage particulier que la décision procure aux transferts de données n'est plus justifié et sera retiré.

3.3 La voie à suivre

Les engagements pris par les États-Unis dans le cadre du «bouclier vie privée» constitueront la base d'une nouvelle décision de la Commission constatant un niveau de protection adéquat, dans laquelle ils seront transcrits. Les entreprises sont encouragées à commencer à se préparer dès maintenant afin d'être en mesure d'adhérer au nouveau cadre dès que possible après sa mise en place, après l'adoption de la décision de la Commission. Pour sa part, le gouvernement américain publiera ses déclarations dans le Registre fédéral des États-Unis, attestant ainsi publiquement qu'il respectera ses engagements.

Le «bouclier vie privée UE-États-Unis» nécessite l'intervention de nombreux acteurs :

- les entreprises américaines participantes qui doivent s'acquitter de leurs obligations découlant du cadre, en sachant pertinemment que celui-ci sera appliqué de manière rigoureuse et qu'elles seront sanctionnées si elles ne s'y conforment pas. Afin d'accroître la confiance de leurs consommateurs, les entreprises sont également encouragées à désigner les autorités de protection des données de l'UE pour régler les plaintes dans le cadre du «bouclier vie privée», car les citoyens européens sont davantage susceptibles de s'adresser à ces autorités. De même, plus les entreprises seront disposées à recourir à la possibilité, conférée par la législation américaine, de publier des rapports de transparence concernant les demandes d'accès, à des fins répressives ou de sécurité nationale, à des données de l'UE que ces entreprises reçoivent, plus les personnes concernées seront convaincues que cet accès est limité à ce qui est nécessaire et proportionné[23];

- les diverses autorités américaines chargées de surveiller et de faire appliquer le cadre, en respectant les limites et les garanties relatives à l'accès aux données à des fins répressives ou de sécurité nationale, et les autorités chargées de répondre, dans les délais et de manière appropriée, aux plaintes des citoyens européens relatives à d'éventuels abus concernant leurs données à caractère personnel;

[23] De tels rapports seraient établis conformément aux dispositions de la loi américaine intitulée «FREEDOM Act» de 2015. Voir la note de bas de page 22.

– les autorités de protection des données de l'UE, qui ont un rôle important à jouer pour que les personnes puissent faire valoir leurs droits conférés par le «bouclier vie privée», notamment en transmettant leurs plaintes aux autorités américaines compétentes et en coopérant avec ces dernières, en saisissant le médiateur, en aidant les plaignants à porter leur affaire devant le Privacy Shield Panel, ainsi qu'en exerçant un contrôle sur les transferts de données en matière de ressources humaines; et

– la Commission, qui est chargée d'émettre des conclusions sur le caractère adéquat du niveau de protection des données et de le réexaminer régulièrement : ces examens réguliers marquent un changement important par rapport à la situation statique antérieure, en transformant l'appréciation du caractère adéquat du «bouclier vie privée» en un cadre vivant et étroitement surveillé.

L'examen conjoint annuel et le rapport consécutif de la Commission – ainsi que la perspective d'une suspension de l'accord en cas de non-respect – joueront donc un rôle déterminant pour que le «bouclier vie privée» résiste à l'épreuve du temps. Notre ambition commune, des deux côtés de l'Atlantique, doit être de développer ensemble une forte culture de respect de la vie privée et de protection des droits individuels, qui rétablisse et maintienne la confiance.

4. L'ACCORD-CADRE: RENFORCER LES GARANTIES EN MATIERE DE PROTECTION DES DONNEES POUR LA COOPERATION ENTRE LES SERVICES REPRESSIFS

4.1 Le contexte

Une dimension importante de notre relation transatlantique est la capacité de l'UE, des États membres et des États-Unis de réagir efficacement aux menaces communes pour la sécurité et de faire face aux défis d'une manière concertée et coordonnée. Cette réaction collective dépend considérablement de notre capacité à échanger des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale. De nombreux accords bilatéraux entre les États membres et les États-Unis et entre l'UE et les États-Unis[24]ont été conclus dans ce sens au fil du temps. Parallèlement, il importe tout autant que ces accords entre services répressifs comportent des garanties effectives en matière de protection des données. Le double objectif de collaborer fructueusement avec nos partenaires américains pour lutter contre la grande criminalité et le terrorisme, tout en faisant progresser le niveau de protection des Européens, conformément à leurs droits fondamentaux et aux règles de protection des données de l'UE, lorsque des transferts sont effectués à ces fins, a été à l'origine des négociations, ouvertes en mars 2011, en vue de la conclusion d'un accord international sur la protection des données dans le domaine répressif, à savoir l'accord-cadre sur la protection des données entre l'UE et les États-Unis[25].

[24] Notamment, l'accord UE-États-Unis sur les données des dossiers passagers (PNR) et le programme UE-États-Unis de surveillance du financement du terrorisme (TFTP).

[25] Un accord entre l'UE et les États-Unis sur la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la

L'Union européenne et les États-Unis ont achevé leurs négociations durant l'été 2015. Les deux parties ont paraphé l'accord-cadre le 8 septembre 2015, au Luxembourg[26], et l'accord est maintenant en attente de ratification des deux côtés de l'Atlantique. Sa signature était cependant subordonnée à l'adoption de la loi sur le recours judiciaire («Judical Redress Act») par le Congrès américain pour offrir, pour la première fois, aux citoyens de l'UE un traitement égal à celui accordé aux citoyens américains par la loi sur la vie privée de 1974 («Privacy Act»)[27]. Le projet de loi a été approuvé par le Congrès le 10 février 2016 et a été promulgué le 24 février 2016.

4.2 Qu'est-ce qui a changé ?

L'accord-cadre consacrera, pour la toute première fois, un ensemble harmonisé et complet de mesures de protection des données qui s'appliqueront à tous les échanges transatlantiques entre les autorités compétentes dans le domaine répressif. C'est, en réalité, un accord en matière de droits fondamentaux qui fixe une norme élevée de protection, à l'aune de laquelle tous les échanges de données prévus dans les accords présents et futurs devront être mesurés.

Premièrement, **les protections et garanties prévues par l'accord-cadre s'appliqueront horizontalement à tous les échanges de données qui auront lieu dans le cadre de la coopération transatlantique des services répressifs en matière pénale**. Cela comprend les transferts en vertu de lois nationales, les accords UE-États-Unis, les accords États Membres-États-Unis (par exemple, les traités d'entraide judiciaire) ainsi que les accords spécifiques prévoyant le transfert de données à caractère personnel par des organismes privés à des fins répressives. Les dispositions convenues augmenteront ainsi immédiatement le niveau de protection garanti aux personnes concernées de l'UE lorsque ces données seront transférées vers les États-Unis. Elles permettront également d'accroître la sécurité juridique pour la coopération policière transatlantique en faisant en sorte que les accords existants contiennent toutes les protections nécessaires et ne soient pas remis en cause dans le cadre de contentieux juridiques.

Deuxièmement, les dispositions couvrent toutes les règles fondamentales de protection des données de l'UE en ce qui concerne les **normes de traitement** (ex. qualité et intégrité des données, sécurité des données, responsabilité et contrôle), **les garanties et les limitations** (ex. limitation des finalités et de l'utilisation, conservation des données, transferts ultérieurs, traitement des données sensibles) ainsi que **les droits des personnes** (accès, rectification, recours administratifs et judiciaires).

---

matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et judiciaire en matière pénale.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

[27] La «Judicial Redress Act» accorde des droits aux ressortissants des «pays couverts» désignés par le gouvernement américain. Ces pays doivent remplir les critères suivants: a) le pays [ou l'organisation régionale] a conclu un accord avec les États-Unis sur la protection de la vie privée pour les informations partagées dans le but de prévenir, de détecter ou de poursuivre des infractions pénales ou enquêter sur celles-ci; b) le pays [ou l'organisation régionale] permet le transfert de données à caractère personnel à des fins commerciales entre lui/elle-même et les États-Unis; et c) les politiques concernant le transfert de données à caractère personnel à des fins commerciales ou à des fins connexes du pays ou de l'organisation régionale ne nuisent pas gravement aux intérêts de la sécurité nationale des États-Unis.

Troisièmement, l'accord garantira le **droit à un recours juridictionnel en cas de refus d'accès, de refus de rectification et de divulgation illicite.** C'est là un progrès majeur qui contribuera grandement à rétablir la confiance dans les échanges transatlantiques. Cette exigence essentielle de l'UE, réclamée de longue date et restée sans réponse pendant de nombreuses années, a déjà été prise en compte dans la «Judicial Redress Act» présentée au Congrès américain en mars 2015 et adoptée le 10 février 2016. Cette loi étendra aux citoyens de l'UE[28] trois voies de recours majeures prévues par la «Privacy Act» de 1974 qui sont, pour le moment, réservées uniquement aux citoyens et résidents permanents aux États-Unis. Ainsi, pour la première fois, les citoyens de l'UE pourront se prévaloir de droits d'application générale pour tout transfert transatlantique de données dans le domaine répressif. On supprime ainsi une inégalité de traitement essentielle entre les citoyens européens et américains.

Quatrièmement, l'accord-cadre généralise et étend à tout le domaine répressif le principe qui veut que **le contrôle indépendant** soit une exigence fondamentale pour la protection des données, principe qui n'est pas présent dans la plupart des accords bilatéraux existants. Cela inclut le pouvoir effectif d'examiner et de statuer sur les plaintes individuelles portant sur le respect de l'accord.

Cinquièmement, la mise en œuvre effective de l'accord-cadre sera soumise à des **vérifications conjointes périodiques**. Une attention particulière sera accordée, lors de ces examens, aux dispositions relatives aux droits des personnes (accès, rectification, recours administratifs et judiciaires).

L'accord-cadre n'autorise pas en soi les transferts de données et ne constitue pas une décision constatant un niveau de protection adéquat.

4.3 La voie à suivre

L'entrée en vigueur de la «Judicial Redress Act»[29] ouvrira la voie à la signature de l'accord-cadre. La Commission soumettra prochainement au Conseil une proposition de décision autorisant la signature de cet accord-cadre. Après la signature, la décision relative à la conclusion de l'accord devra être adoptée par le Conseil, après avoir obtenu le consentement du Parlement européen. L'accord-cadre améliorera sensiblement la situation actuelle, qui se caractérise par des règles de protection des données fragmentées, non harmonisées et souvent faibles, éparpillées dans une mosaïque d'instruments multilatéraux, bilatéraux, nationaux et sectoriels. L'accord-cadre a un effet rétroactif en ce qu'il complétera les garanties relatives à la protection des données stipulées dans les accords en vigueur lorsque et dans la mesure où celles-ci n'atteignent pas le niveau de garantie requis. À cet égard, il apportera une valeur ajoutée significative en «comblant les lacunes» des accords existants qui prévoient des normes de protection des données moins élevées que celles présentes dans l'accord-cadre. Il assurera ainsi la continuité de la coopération des services répressifs tout en garantissant une

[28] Selon la «Judicial Redress Act», d'autres pays tiers ou «organisations régionales d'intégration économique» peuvent également être désignés comme «pays couverts», ce qui aurait pour effet de faire bénéficier leurs ressortissants de droits de recours juridictionnel.

[29] La «Judical Redress Act» entre en vigueur 90 jours après sa promulgation.

sécurité juridique accrue lorsque les transferts seront effectués. En ce qui concerne les futurs accords, l'accord-cadre représentera un filet de sécurité en-dessous duquel le niveau de protection ne pourra pas descendre. Il s'agit d'une garantie très importante pour l'avenir et d'un changement majeur par rapport à la situation actuelle où les garanties, les protections et les droits doivent être renégociés pour chaque nouvel accord. L'accord-cadre constitue donc un modèle contenant les garanties types qui ne peuvent pas être négociées à la baisse. Il crée un précédent essentiel, non seulement pour les relations entre l'UE et les États-Unis mais, plus généralement, pour tout accord international futur concernant la protection ou l'échange de données.

Négocié parallèlement à la réforme, l'accord-cadre est en conformité avec l'acquis de l'UE en matière de protection des données. Son interaction avec la directive sur la police est particulièrement pertinente, compte tenu de l'importance d'avoir un niveau élevé et commun de protection des données, que les données personnelles soient traitées au niveau national ou échangées au-delà des frontières, au sein de l'UE ou avec des pays tiers. À cet égard, l'accord-cadre contribuera à justifier les prescriptions générales de la réforme dans le contexte transatlantique.

La conclusion des négociations sur l'accord-cadre, qui fixe des normes communes dans un domaine complexe du droit et de la politique, constitue une réalisation majeure. Le futur accord-cadre rétablira et renforcera la confiance, il garantira la légalité des transferts de données et il facilitera la coopération entre l'UE et les États-Unis dans ce domaine.

Pour aller plus loin, il est nécessaire de relever ensemble les défis communs dans le domaine de la coopération policière et judiciaire. Une question importante reste posée, celle de l'accès direct des autorités répressives aux données à caractère personnel détenues par les entreprises privées à l'étranger. Cet accès devrait, en principe, avoir lieu dans le cadre des canaux formels de la coopération, tels que les accords d'entraide judiciaire ou d'autres accords sectoriels. Les entreprises privées sont actuellement exposées à une insécurité juridique qui pourrait avoir une incidence sur leur capacité d'exercer des activités à l'étranger, si on leur demande de donner accès à une preuve électronique régie par le droit d'un pays pour des données à caractère personnel régies par le droit d'un autre pays. Parallèlement au prochain réexamen de l'accord d'entraide judiciaire entre l'UE et les États-Unis[30], l'UE souhaiterait avoir de plus amples échanges avec les États-Unis sur cette question, notamment au sujet de l'élaboration de règles communes et plus efficaces pour la collecte de preuves électroniques.

5. CONCLUSION

La conclusion fructueuse des actions clés définies dans la communication de 2013 démontre la capacité de l'UE de résoudre des problèmes de manière pragmatique et réfléchie, sans pour autant sacrifier ses droits fondamentaux, ses valeurs et ses traditions solides. Elle montre également que l'UE et les États-Unis sont capables d'aplanir leurs différends et de prendre des

[30] Décision 2009/820/PESC du Conseil du 23 octobre 2009 concernant la conclusion, au nom de l'Union européenne, de l'accord d'extradition entre l'Union européenne et les États-Unis d'Amérique et de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique, JO L 291 du 7.11.2009, p. 40-41.

décisions difficiles afin de préserver une relation stratégique qui a résisté à l'épreuve du temps. Cependant, à l'heure où nous entamons un nouveau chapitre de nos relations bilatérales, nous devons maintenir notre vigilance car nous continuons à faire face à des menaces et des défis communs dans un monde incertain.

Une fois le «bouclier vie privée» et l'accord-cadre en place, il incombera aux deux parties de faire en sorte que ces deux grands cadres régissant les transferts de données fonctionnent efficacement et durablement. Leur succès dépendra en grande partie de la bonne application et du respect des droits accordés aux personnes. Il dépendra également de l'évaluation continue de leur fonctionnement. Il faudra pour cela passer d'un état d'esprit statique à un processus plus dynamique.

Dans ce contexte, un élément essentiel de ce processus est lié à la réforme en cours des programmes de renseignement américains. À cet égard, la Commission étudiera attentivement les prochains rapports du Privacy and Civil Liberties Oversight Board (conseil de surveillance de la vie privée et des libertés civiles) et le réexamen du programme de surveillance au titre de l'article 702 de la loi sur la surveillance et le renseignement étranger (loi FISA), attendu en 2017. En particulier, les réformes supplémentaires relatives à la transparence, au contrôle et à l'extension des garanties aux personnes n'ayant pas la nationalité américaine seront suivies de près.

Plus généralement, étant donné l'importance des flux de données transfrontaliers pour le commerce transatlantique, l'UE suivra avec intérêt les prochaines avancées de la législation américaine dans le domaine de la vie privée. Maintenant que l'Europe s'est dotée d'un corps de règles unique, cohérent et solide, nous espérons que les États-Unis poursuivront, eux aussi, leurs efforts pour arriver à un régime complet de protection de la vie privée et des données. C'est grâce à une telle démarche globale que la convergence entre les deux régimes pourrait être atteinte à plus long terme. À ce sujet, la Commission organisera un sommet annuel sur la vie privée avec les ONG intéressées et d'autres parties prenantes concernées des deux côtés de l'Atlantique.

Le partenariat UE-États-Unis peut être un moteur de développement et de promotion des normes juridiques internationales qui protègent la vie privée et les données à caractère personnel. Les initiatives au niveau de l'ONU, notamment les travaux du Rapporteur spécial sur le droit à la vie privée, peuvent également jouer un rôle important à cet égard. Dans les années à venir, compte tenu de l'actualité croissante de ces questions sur la scène internationale, l'Union européenne et les États-Unis devraient saisir cette occasion de faire progresser, dans l'environnement numérique mondialisé, leurs valeurs communes en matière de droits et de libertés individuelles.