COMMISSION
EUROPÉENNE

Bruxelles, le 10.1.2017
COM(2017) 7 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Échange et protection de données à caractère personnel à l'ère de la mondialisation

1. INTRODUCTION

La protection des données à caractère personnel fait partie des fondements constitutionnels communs de l'Europe et est consacrée à l'article 8 de la charte des droits fondamentaux de l'UE. Elle occupe une place centrale dans la législation de l'UE depuis plus de vingt ans, de l'adoption de la directive sur la protection des données en 1995[1] (la «directive de 1995») à celle du règlement général sur la protection des données (RGPD)[2] et de la directive «police»[3] en 2016.

Comme l'a souligné le président Juncker dans son discours du 14 septembre 2016 sur l'état de l'Union, «*[êt]re européen, c'est avoir le droit de voir ses données à caractère personnel protégées par une législation forte, une législation européenne. [...] Car en Europe, la vie privée n'est pas un vain mot. C'est une question de dignité humaine.*»

La demande de protection des données à caractère personnel ne se limite toutefois pas à l'Europe. Les consommateurs du monde entier accordent une valeur de plus en plus importante au respect de leur vie privé. Les entreprises reconnaissent pour leur part qu'une forte protection de la vie privée leur offre un avantage concurrentiel dans la mesure où la confiance dans leurs services se renforce. Elles sont nombreuses, en particulier celles de dimension mondiale, à aligner leurs politiques de protection de la vie privée sur le RGPD, à la fois parce qu'elles veulent exercer leurs activités dans l'UE et parce qu'elles considèrent ce règlement comme un modèle à suivre.

De même, plusieurs pays et organisations régionales extérieurs à l'UE, de notre voisinage immédiat à l'Asie, l'Amérique latine et l'Afrique, adoptent de nouvelles législations en matière de protection des données ou actualisent leurs législations existantes afin d'exploiter les possibilités offertes par l'économie numérique mondiale et de répondre à la demande croissante d'un renforcement de la sécurité des données et de la protection de la vie privée. Bien que les approches et le niveau d'avancement législatif varient d'un pays à l'autre, il existe des indices d'une plus grande convergence vers d'importants principes en matière de protection des données, en particulier dans certaines régions du monde[4]. Une compatibilité accrue entre les différents systèmes de protection des données faciliterait les flux internationaux de données à caractère personnel, tant à des fins commerciales que dans le cadre d'une coopération entre autorités publiques (par exemple, autorités chargées de faire

---

1 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 23.11.1995.

2 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1. Entré en vigueur le 24 mai 2016, il sera applicable à partir du 25 mai 2018.

3 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89). Elle est entrée en vigueur le 5 mai 2016. Les États membres ont jusqu'au 6 mai 2018 pour la transposer dans leur législation nationale.

4 Voir «Data protection regulations and international data flows: Implications for trade and development», CNUCED (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

appliquer la loi). L'UE doit saisir cette occasion de promouvoir ses valeurs en matière de protection des données et de faciliter les flux de données en encourageant une convergence des systèmes juridiques. Comme annoncé dans le programme de travail de la Commission[5], la présente communication définit donc le cadre stratégique de la Commission pour les «décisions d'adéquation» ainsi que d'autres outils applicables aux transferts de données et aux instruments internationaux de protection des données.

2. LE TRAIN DE MESURES DE L'UE VISANT À RÉFORMER LA PROTECTION DES DONNÉES - UN CADRE LÉGISLATIF MODERNE CONFÉRANT UN HAUT NIVEAU DE PROTECTION AUX FLUX INTERNATIONAUX DE DONNÉES

La réforme de la législation de l'UE en matière de protection des données qui a été adoptée en avril 2016 met en place un système qui garantit un haut niveau de protection tout en étant ouvert aux possibilités offertes par la société de l'information mondiale. En permettant aux citoyens d'exercer un contrôle accru sur leurs données à caractère personnel, la réforme renforce la confiance des consommateurs dans l'économie numérique. En harmonisant et en simplifiant l'environnement juridique, elle facilite et rend moins contraignant l'exercice des activités des entreprises nationales et étrangères dans l'UE, y compris au moyen de flux internationaux de données. L'UE allie aujourd'hui une ouverture aux flux internationaux de données au plus haut niveau de protection offert aux citoyens. Elle a le potentiel pour devenir un centre de services de données nécessitant confiance et libre circulation des données.

2.1 Un cadre européen de protection des données global, unifié et simplifié

La réforme de l'UE établit un cadre global régissant le traitement des données à caractère personnel à la fois dans les secteurs public et privé et dans les domaines répressif et du commerce (la directive «police» et le RGPD, respectivement).

En application du RGPD, les 28 législations nationales actuelles laisseront la place à un ensemble paneuropéen unique de règles à partir de mai 2018. Grâce au mécanisme de guichet unique nouvellement créé, une autorité chargée de la protection des données («APD») aura pour tâche de superviser les opérations de traitement transfrontière de données réalisées par une entreprise dans l'UE. Une interprétation cohérente des nouvelles règles sera garantie. Pour les opérations transfrontières impliquant plusieurs APD nationales, une décision unique sera adoptée de manière à apporter des solutions communes aux problèmes communs. En outre, le RGPD établit une égalité de traitement entre les entreprises de l'UE et les entreprises étrangères dans la mesure où les entreprises établies hors de l'UE devront appliquer les mêmes règles que les entreprises européennes si elles offrent des biens et des services ou surveillent le comportement de personnes dans l'Union. Une confiance accrue des consommateurs sera bénéfique à la fois pour les opérateurs commerciaux de l'UE et pour ceux de pays tiers.

La directive «police» établit des règles communes pour le traitement des données à caractère personnel des personnes impliquées dans des procédures pénales, qu'il s'agisse de suspects,

[5] Programme de travail de la Commission pour 2017, Répondre aux attentes - Pour une Europe qui protège, donne les moyens d'agir et défend», COM(2016) 710 final du 25.10.2016, p. 12 et annexe 1.

de victimes ou de témoins, tout en tenant compte de la spécificité du domaine de la police et de la justice pénale. L'harmonisation des règles de protection des données dans le domaine répressif, y compris des règles relatives aux transferts internationaux, facilitera la coopération transfrontière entre les autorités policières et judiciaires, tant à l'intérieur de l'UE qu'avec les partenaires internationaux, et créera ainsi les conditions propices à une lutte plus efficace contre la criminalité. Il s'agit d'une contribution importante au programme européen en matière de sécurité[6].

2.2 Une panoplie d'instruments renouvelée et diversifiée pour les transferts internationaux

Depuis sa conception, la législation de l'UE en matière de protection des données a prévu plusieurs mécanismes permettant les transferts internationaux de données. Ces règles visent principalement à ce que, lorsque les données à caractère personnel d'Européens sont transférées à l'étranger, celles-ci continuent de bénéficier du même niveau de protection. Au fil des ans, ces règles ont constitué la norme applicable aux flux internationaux de données au sein de nombreuses juridictions. Si l'architecture reste substantiellement la même que celle de la directive de 1995, la réforme des règles relatives aux transferts internationaux clarifie et simplifie leur usage et introduit de nouveaux outils pour les transferts.

En vertu du droit de l'UE, le transfert de données à caractère personnel à l'étranger peut reposer sur une «décision d'adéquation» de la Commission, établissant qu'un pays tiers fournit un niveau de protection des données qui est «substantiellement équivalent»[7] à celui garanti au sein de l'UE. Une telle décision permet la libre circulation des données à caractère personnel vers ce pays tiers sans que l'exportateur des données n'ait à fournir des garanties supplémentaires ou à obtenir une quelconque autorisation. Un catalogue précis et détaillé d'éléments que la Commission doit prendre en compte lorsqu'elle évalue le caractère adéquat de la protection d'un système étranger est à la disposition des pays ou des organisations internationales intéressés[8]. À présent, la Commission peut aussi adopter des décisions d'adéquation dans le domaine répressif[9]. En outre, la réforme, qui s'appuie sur les pratiques relevant de la directive de 1995, prévoit explicitement une évaluation du caractère adéquat de

---

6 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.

7 Arrêt de la Cour de justice de l'UE du 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems contre Data Protection Commissioner*, points 73, 74 et 96. Voir également le considérant 104 du RGPD et le considérant 67 de la directive «police», qui font référence à la norme d'équivalence essentielle.

8 Voir l'article 45 du RGPD. Conformément à l'article 45, paragraphe 2, dans son évaluation, la Commission doit notamment tenir compte de l'état de droit, du respect des droits de l'homme et des libertés fondamentales, de la législation pertinente, y compris en ce qui concerne la protection des données, la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que de l'accès des autorités publiques aux données à caractère personnel. Ceux-ci doivent reposer sur des droits effectifs et opposables, y compris les recours administratifs et judiciaires que peuvent introduire les personnes concernées, et sur le fonctionnement effectif d'une autorité de contrôle indépendante chargée d'assurer le respect des règles en matière de protection des données et de les faire appliquer. L'adhésion à des conventions juridiquement contraignantes, en particulier la Convention n° 108 du Conseil de l'Europe, et la participation à des systèmes multilatéraux ou régionaux de protection des données, seront également prises en compte.

9 Voir l'article 36, paragraphe 2, de la directive «police» pour les aspects spécifiques de l'évaluation du caractère adéquat de la protection.

la protection offerte sur un territoire particulier d'un pays tiers ou dans un secteur particulier d'un pays tiers (l'«adéquation partielle»)[10].

En l'absence de décision d'adéquation, les transferts internationaux peuvent se fonder sur plusieurs autres outils de transfert offrant des garanties appropriées en matière de protection des données.[11] La réforme formalise et étend les possibilités d'utiliser les instruments existants tels que les clauses contractuelles types (CCT)[12] et les règles d'entreprise contraignantes (REC)[13]. Par exemple, des CCT peuvent à présent être insérées dans un contrat conclu entre des sous-traitants de l'UE et des sous-traitants d'un pays tiers (les clauses types «de sous-traitant à sous-traitant»)[14]. Pour ce qui est des REC, qui étaient limitées jusqu'à présent à des arrangements entre entités du même groupe d'entreprises, elles peuvent désormais être utilisées par un ensemble d'entreprises qui participent à une activité économique conjointe, mais ne font pas nécessairement partie du même groupe[15]. La réforme réduit également les contraintes administratives en supprimant l'exigence générale de notification préalable aux APD de transferts de données vers un pays tiers sur la base de CCT ou de REC, ainsi que l'exigence générale d'autorisation de tels transferts par ces APD[16]. Il s'agit d'une simplification importante du système de transferts internationaux de données de l'UE, car l'existence de ces exigences, qui varient actuellement d'un État membre à l'autre, est souvent perçue comme un obstacle significatif aux flux de données, en particulier pour les petites entreprises[17].

En outre, la réforme introduit de nouveaux instruments pour les transferts internationaux[18]. Les responsables du traitement et les sous-traitants pourront utiliser, à certaines conditions[19], des codes de conduite ou des mécanismes de certification approuvés (tels que les labels ou les marques de protection de la vie privée) afin d'établir des «garanties appropriées». Cela devrait permettre l'élaboration de solutions plus adaptées aux transferts internationaux qui prennent en compte, par exemple, les caractéristiques et les besoins particuliers d'entreprises ou d'un secteur donnés ou de flux de données particuliers. La réforme offre également la possibilité de prévoir des garanties appropriées pour les transferts de données entre autorités ou organismes

---

10 Voir l'article 45, paragraphe 1, du RGPD, et l'article 36, paragraphe 1, de la directive «police».

11 Voir par exemple 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 du 6.11.2015.

12 Les CCT énoncent les obligations en matière de protection des données respectives de l'exportateur de l'UE et de l'importateur du pays tiers.

13 Les REC sont des règles internes adoptées par un groupe d'entreprises multinational afin de procéder à des transferts au sein du même groupe d'entreprises vers des entités établies dans des pays qui n'offrent pas un niveau de protection adéquat. Si les REC sont déjà utilisées dans le cadre de la directive de 1995, le RGPD codifie et formalise leur rôle en tant qu'outil de transfert.

14 Voir l'article 46, paragraphe 2, points c) et d), et le considérant 168 du RGPD.

15 Voir l'article 46, paragraphe 2, point b), l'article 47 et le considérant 110 du RGPD.

16 Voir l'article 46, paragraphe 2, du RGPD.

17 Le fait que ces obligations d'enregistrement constituent un obstacle aux échanges pour de nombreuses entreprises, en particulier les PME, a été souligné notamment dans le rapport de la CNUCED, p. 34.

18 Voir l'article 46, paragraphe 2, points e) et f), du RGPD.

19 Les responsables du traitement hors UE pourront adhérer à un code de conduite ou à un mécanisme de certification de l'UE en prenant l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres juridiquement contraignants, d'appliquer les garanties de protection des données figurant dans ces instruments. Voir l'article 42, paragraphe 2, du RGPD.

publics, sur la base d'accords internationaux ou d'arrangements administratifs[20]. Enfin, le RGPD clarifie le recours aux «dérogations»[21] (par exemple, le consentement de la personne concernée, l'exécution d'un contrat ou des motifs importants d'intérêt public) sur lesquelles des entités peuvent, dans certaines situations, fonder leurs transferts de données en l'absence de décision d'adéquation et indépendamment de l'utilisation de l'un des instruments précités. Il contient en particulier une dérogation nouvelle, quoique limitée, relative aux transferts qui peuvent avoir lieu aux fins des intérêts légitimes d'une entreprise[22].

Enfin, la réforme donne à la Commission les moyens d'élaborer des mécanismes de coopération internationale destinés à faciliter l'application des règles en matière de protection des données, y compris au moyen d'accords d'assistance mutuelle[23]. Il s'agit d'une reconnaissance de la contribution que des formes de coopération plus étroite entre des autorités de contrôle au niveau international pourraient apporter afin de garantir à la fois une protection plus effective des droits des personnes et une sécurité juridique accrue pour les entreprises.

3. TRANSFERTS INTERNATIONAUX DE DONNÉES DANS LE SECTEUR COMMERCIAL: FACILITER LES ÉCHANGES TOUT EN PROTÉGEANT LA VIE PRIVÉE

Le respect de la vie privée est une condition préalable à des flux commerciaux mondiaux stables, sûrs et compétitifs. La vie privée n'est pas un produit négociable[24]. L'internet et la numérisation des biens et des services ont transformé l'économie mondiale et le transfert par-delà les frontières de données, y compris à caractère personnel, fait partie des opérations courantes des entreprises européennes de toutes tailles et de tous secteurs d'activité. Les échanges commerciaux reposant de plus en plus sur des flux de données à caractère personnel, la confidentialité et la sécurité de ce type de données sont devenues essentielles à la confiance des consommateurs. Ainsi, deux tiers des Européens se disent préoccupés par le fait de n'avoir aucun contrôle sur les informations qu'ils communiquent en ligne, tandis que la moitié des personnes interrogées craignent d'être un jour victimes d'une fraude[25]. Parallèlement, les entreprises européennes opérant dans certains pays tiers sont de plus en plus confrontées à des restrictions protectionnistes qui ne peuvent être justifiées par des considérations légitimes de protection de la vie privée.

À l'ère du numérique, la promotion de niveaux élevés de protection des données doit nécessairement aller de pair avec une facilitation des échanges commerciaux internationaux. Si la protection des données à caractère personnel n'est pas négociable[26] dans les accords commerciaux, le régime de l'UE applicable aux transferts internationaux de données, tel qu'il

---

20 Voir l'article 46, paragraphe 2, point a), et l'article 46, paragraphe 3, point b), du RGPD.
21 Voir l'article 49 du RGPD.
22 Voir l'article 49, paragraphe 1, deuxième alinéa.
23 Voir l'article 50 du RGPD.
24 Voir par exemple la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Le commerce pour tous - Vers une politique de commerce et d'investissement plus responsable, COM(2015) 497 final du 14.10.2015, p. 7.
25 Eurobaromètre spécial 431 sur la protection des données, juin 2015.
26 Orientations politiques du président Juncker: *Un nouvel élan pour l'Europe : mon programme pour l'emploi, la croissance, l'équité et le changement démocratique.*

est décrit plus haut, fournit une panoplie d'instruments étendue et variée qui permet des flux de donnés dans diverses situations tout en assurant un niveau élevé de protection.

3.1 Décisions d'adéquation

Un constat d'adéquation permet la libre circulation de données à caractère personnel à partir de l'UE, sans que l'exportateur de données de l'Union ne doive mettre en œuvre des garanties supplémentaires, ni se soumettre à de nouvelles conditions. En concluant que l'ordre juridique du pays concerné offre un niveau de protection adéquat, la décision reconnaît que le système de ce pays est proche de celui des États membres de l'UE. Il en résulte que les transferts vers le pays en question seront assimilés à des transferts de données intra-UE, ce qui permettra d'offrir un accès privilégié au marché unique de l'UE tout en ouvrant des canaux commerciaux pour les opérateurs de l'UE. Comme indiqué plus haut, une telle reconnaissance exige nécessairement un niveau de protection comparable (ou «substantiellement équivalent»)[27] à celui garanti au sein de l'Union. Elle implique une évaluation globale du système du pays tiers, y compris de ses règles régissant l'accès des autorités publiques aux données à caractère personnel à des fins d'application de la loi, de sécurité nationale ou à d'autres fins d'intérêt général.

Dans le même temps, ainsi que l'a confirmé la Cour de justice dans l'arrêt *Schrems* en 2015, le principe d'adéquation n'exige pas que l'on reproduise à l'identique les règles de l'UE[28]. Il s'agit plutôt de déterminer si le système étranger concerné offre, dans son ensemble, par l'essence de ses droits en matière de protection de la vie privée et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau élevé requis de protection. Comme l'ont montré les décisions d'adéquation adoptées jusqu'à présent, la Commission est en mesure de reconnaître le caractère adéquat d'une variété de systèmes de protection de la vie privée représentant diverses traditions juridiques. Ces décisions concernent des pays qui sont étroitement intégrés dans l'Union européenne et ses États membres (Suisse, Andorre, Îles Féroé, Guernesey, Jersey, Île de Man), d'importants partenaires commerciaux (Argentine, Canada, Israël, États-Unis) et des pays jouant un rôle précurseur dans l'élaboration de lois en matière de protection des données dans leurs régions respectives (Nouvelle Zélande, Uruguay).

Les décisions concernant le Canada et les États-Unis sont des constats d'adéquation «partiels». La décision relative au Canada s'applique uniquement aux entités privées relevant de la loi canadienne sur la protection des renseignements personnels et les documents électroniques. La décision adoptée récemment sur le bouclier de protection des données UE-États-Unis[29] constitue un cas particulier dans la mesure où, en l'absence de législation générale en matière de protection des données aux États-Unis[30], elle se fonde sur les

---

27 Voir la note de bas de page n° 7.

28 Voir le point 74 de l'arrêt *Schrems*.

29 Décision d'exécution (UE) 2016/1260 du 12 juillet 2016.

30 La Commission encourage les États-Unis à poursuivre leurs efforts en vue de la mise en place d'un système global de protection de la vie privée et des données, ce qui permettrait de parvenir à plus long terme à une convergence entre les deux systèmes. Voir la communication de la Commission au Parlement européen et au

engagements pris par les entreprises participantes d'appliquer les normes élevées en matière de protection des données énoncées par ce dispositif, lesquelles sont exécutoires en vertu de la législation américaine. En outre, le bouclier de protection s'appuie sur les déclarations et les garanties spécifiques formulées par les autorités américaines en ce qui concerne l'accès aux données à des fins de sécurité nationale[31], qui étayent le constat d'adéquation. Le respect de ces engagements sera suivi de près par la Commission et sera intégré dans l'examen annuel du fonctionnement du cadre.

Ces dernières années, de nouvelles législations dans le domaine de la protection des données et du respect de la vie privée ont été adoptées par de plus en plus de pays dans le monde ou sont en cours d'adoption. En 2015, le nombre de pays à avoir adopté de telles législations s'élevait à 109, un chiffre en forte hausse par rapport aux 76 pays recensés à la mi-2011[32]. De surcroît, environ 35 pays préparent actuellement des lois en matière de protection des données[33]. Ces lois nouvelles ou révisées tendent à se fonder sur un noyau de principes communs, parmi lesquels la reconnaissance de la protection des données comme un droit fondamental, l'adoption d'une législation globale dans ce domaine, l'existence de droits au respect de la vie privée opposables et la mise en place d'une autorité de contrôle indépendante. Une telle évolution offre de nouvelles possibilités de continuer à faciliter les flux de données tout en garantissant un niveau constamment élevé de protection des données à caractère personnel, notamment au moyen des constats d'adéquation.

En vertu de la législation de l'UE, un constat d'adéquation requiert l'existence de règles en matière de protection des données qui soient comparables à celles de l'Union[34]. Cela concerne tant les protections de fond applicables aux données à caractère personnel que les mécanismes correspondants de contrôle et de recours disponibles dans le pays tiers.

En vertu de son cadre relatif aux constats d'adéquation, la Commission considère qu'il y a lieu de prendre en compte les critères exposés ci-après lorsqu'elle détermine les pays tiers avec lesquels il conviendrait de mener un dialogue sur le caractère adéquat de la protection[35]:

(i) l'étendue des relations commerciales (existantes ou potentielles) de l'UE avec un pays tiers donné, y compris l'existence d'un accord de libre-échange ou de négociations en cours;

Conseil - Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides, COM(2016) 117 final du 29.2.2016.

31 Cela implique notamment l'application de la directive présidentielle n° 28 (PPD-28), qui impose un certain nombre de limitations et de garanties pour les opérations de «renseignement d'origine électromagnétique», et la désignation d'un médiateur spécifiquement chargé de traiter les plaintes introduites par des citoyens de l'UE à cet égard.

32 G. Greenleaf, «Global data privacy laws 2015: 109 countries, with European laws now in a minority», (2015) 133 Privacy Laws & Business International Report, 14-17.

33 Étude de la CNUCED, p. 8 et 42 (voir note de bas de page n° 4 plus haut).

34 À cet égard, la Commission tient également compte des obligations incombant au pays tiers en vertu de conventions juridiquement contraignantes, en particulier de son adhésion à la Convention n° 108 et à son protocole additionnel, lorsqu'elle évalue le caractère adéquat de la protection. Voir l'article 45, paragraphe 2, point c), et le considérant 105 du RGPD.

35 Pour les pays avec lesquels une coopération en matière répressive et de sécurité intérieure présente un grand intérêt, la Commission envisagera la possibilité d'émettre des constats d'adéquation dans le cadre de la directive «police» (voir point 4).

(ii) l'étendue des flux de données à caractère personnel provenant de l'UE, preuve de liens géographiques et/ou culturels;

(iii) le rôle précurseur du pays tiers dans le domaine de la protection de la vie privée et des données, qui peut servir de modèle pour d'autres pays de sa région[36]; et

(iv) la relation politique globale avec le pays tiers concerné, en particulier dans le contexte de la promotion de valeurs communes et d'objectifs partagés au niveau international.

Sur la base de ces considérations, la Commission entretiendra un dialogue actif avec des partenaires commerciaux importants d'Asie de l'Est et du Sud-Est, à commencer par le Japon et la Corée en 2017[37], et avec l'Inde pour autant qu'elle ait avancé dans la modernisation de sa législation en matière de protection des données, ainsi qu'avec des pays d'Amérique latine, en particulier du Mercosur, et du voisinage européen qui se sont montrés désireux d'obtenir un «constat d'adéquation». En outre, la Commission se félicite des manifestations d'intérêt émanant d'autres pays tiers qui souhaitent engager un dialogue sur ces questions. Les discussions relatives à un éventuel constat d'adéquation prennent la forme d'un dialogue bilatéral qui implique de fournir toutes les clarifications nécessaires sur les règles de l'UE en matière de protection des données et d'examiner les moyens de renforcer la convergence des lois et des pratiques des pays tiers.

Dans certaines situations, plutôt que d'adopter une approche nationale, il pourrait être plus indiqué de recourir à d'autres options telles qu'une décision d'adéquation partielle ou sectorielle (par exemple, pour les secteurs des services financiers ou des technologies de l'information), qui porterait sur des zones géographiques ou des secteurs d'activité représentant une partie importante de l'économie d'un pays tiers donné. De telles options devront être envisagées à la lumière d'éléments tels que, par exemple, la nature et l'état d'avancement du régime de protection de la vie privée (loi unique, lois multiples ou sectorielles, etc.), la structure constitutionnelle du pays tiers ou la question de savoir si certains secteurs de l'économie sont particulièrement exposés à des flux de données provenant de l'UE.

L'adoption d'une décision d'adéquation implique l'ouverture d'un dialogue spécifique et des formes de coopération étroite avec le pays tiers concerné. Les décisions d'adéquation sont des documents évolutifs qui doivent faire l'objet d'un suivi étroit de la Commission et être adaptés en cas d'évolution ayant un effet sur le niveau de protection garanti par le pays tiers en question[38]. À cette fin, des examens périodiques (au moins tous les quatre ans) seront organisés afin de remédier aux problèmes émergents et d'échanger de bonnes pratiques entre

[36] Ce critère peut être particulièrement pertinent pour les pays en développement et en transition car la protection des données à caractère personnel est à la fois un élément central de l'état de droit et un facteur important de la compétitivité économique.

[37] Le Japon et la Corée ont récemment adopté ou modernisé leur législation afin de mettre en place des régimes globaux de protection des données.

[38] En vertu de l'article 45, paragraphes 4 et 5, du RGPD, la Commission suit en permanence l'évolution de la situation dans les pays tiers et est habilitée à abroger, modifier ou suspendre une décision d'adéquation si elle considère que le pays concerné ne garantit plus un niveau de protection adéquat.

proches partenaires[39]. Cette approche dynamique s'applique également aux décisions d'adéquation préexistantes qui ont été adoptées en vertu de la directive de 1995 et qui devront être réexaminées si elles ne répondent plus à la norme applicable[40]. Les pays tiers concernés sont donc invités à informer la Commission de toute modification pertinente de leur législation ou de leurs pratiques depuis l'adoption de la décision les concernant. Une telle démarche est essentielle pour garantir la continuité de ces décisions sur la base des nouvelles règles de la réforme[41].

Les règles de l'UE en matière de protection des données ne peuvent être négociées dans le cadre d'un accord de libre-échange[42]. Si les dialogues relatifs à la protection des données et les négociations commerciales avec les pays tiers doivent suivre des voies distinctes, une décision d'adéquation, même partielle ou sectorielle, est le meilleur moyen d'instaurer la confiance mutuelle, ce qui garantit des flux sans entrave de données à caractère personnel et facilite les échanges commerciaux impliquant des transferts de données à caractère personnel vers le pays tiers en question. De telles décisions sont donc de nature à faciliter les négociations commerciales ou peuvent compléter les accords commerciaux existants de manière à amplifier leurs bienfaits. Dans le même temps, en favorisant la convergence des niveaux de protection garantis dans l'UE et le pays tiers, un constat d'adéquation réduit le risque que ce pays invoque des motifs de protection de données à caractère personnel pour imposer des exigences injustifiées en matière de localisation ou de stockage des données. En outre, ainsi qu'elle l'a indiqué dans sa communication intitulée «Le commerce pour tous», la Commission s'efforcera d'utiliser les accords commerciaux de l'UE afin de fixer des règles pour le commerce électronique et les flux de données transfrontières et de s'attaquer aux nouvelles formes de protectionnisme numérique, dans le plein respect et sans préjudice des règles de l'UE sur la protection des données[43].

---

39 Article 45, paragraphe 3, du RGPD.

40 L'article 97, paragraphe 2, point a), du RGPD dispose également que la Commission doit soumettre un rapport d'évaluation au Parlement européen et au Conseil d'ici 2020.

41 Afin de tirer les enseignements de l'arrêt *Schrems*, selon lequel la Commission a outrepassé ses compétences en limitant le pouvoir des APD de suspendre ou d'interdire des flux de données dans la décision relative à la sphère de sécurité, la Commission a adopté, le 16 décembre 2016, une décision modificative «omnibus» supprimant des dispositions similaires dans les décisions d'adéquation existantes et les remplaçant par des dispositions prévoyant uniquement des obligations d'information entre les États membres et la Commission lorsqu'une APD suspend ou interdit des transferts vers un pays tiers. La décision omnibus introduit également l'obligation pour la Commission de suivre les évolutions pertinentes dans le pays tiers. Voir JO L 355 du 17.12.2016, p. 83.

42 Concrètement, un constat d'adéquation est une décision d'exécution unilatérale de la Commission qui est adoptée conformément à la législation de l'UE en matière de protection de données et se fonde sur les critères y figurant.

43 Voir la communication «Le commerce pour tous», p. 12 (voir note de bas de page n° 24 plus haut).

La Commission entend:

- accorder la priorité aux discussions relatives à la possibilité d'adopter des décisions d'adéquation avec d'importants partenaires commerciaux de l'Asie de l'Est et du Sud-Est, à commencer par le Japon et la Corée en 2017, mais également avec d'autres partenaires stratégiques tels que l'Inde, ainsi qu'avec des pays d'Amérique latine, en particulier du Mercosur, et du voisinage européen;

- assurer un suivi étroit du fonctionnement des décisions d'adéquation existantes. Cela implique en particulier de mettre en œuvre le cadre du bouclier de protection des données UE/États-Unis, notamment dans le cadre du réexamen annuel conjoint;

- collaborer avec les pays désireux d'adopter une législation forte en matière de protection des données et assister ceux-ci dans ce processus, et soutenir la convergence de ces pays vers les principes de protection des données de l'UE.

3.2 AUTRES MÉCANISMES DE TRANSFERT DE DONNÉES

Les règles de l'UE en matière de protection des données ont toujours reconnu qu'il n'existe pas d'approche universelle des transferts internationaux de données. C'est d'autant plus vrai en ce qui concerne les règles découlant de la réforme. S'il est vrai que seuls les pays tiers qui remplissent les critères pertinents pourront obtenir des constats d'adéquation, le RGPD prévoit toute une série de mécanismes qui sont suffisamment souples pour s'adapter à une variété de situations de transfert différentes. Des instruments peuvent être mis au point pour tenir compte des conditions ou des besoins particuliers de certains secteurs, modèles commerciaux et/ou opérateurs. Il pourrait s'agir, par exemple, de CCT ciblées sur les exigences d'un secteur particulier, comme des garanties spécifiques pour le traitement de données sensibles dans le secteur de la santé, ou d'un type particulier d'activités de traitement courantes dans certains pays tiers, comme des services d'externalisation effectués pour les entreprises européennes. Cela pourrait se faire soit en adoptant de nouvelles séries de clauses types soit en complétant celles qui existent déjà au moyen de garanties supplémentaires qui pourraient aller de solutions techniques à des solutions organisationnelles en passant par des solutions liées au modèle commercial[44]. Certains besoins sectoriels peuvent également être satisfaits au moyen de REC applicables à des groupes d'entreprises exerçant une activité économique conjointe, par exemple dans le secteur du voyage. Les transferts internationaux entre sous-traitants pourraient profiter de la mise au point de CCT de sous-traitant à sous-traitant ou/et de REC pour les sous-traitants. Enfin, de nouveaux mécanismes de transfert tels que les codes de conduite approuvés et les certifications établies par des tiers agréés offrent aux entreprises la possibilité de mettre en place des solutions sur mesure pour les transferts internationaux tout en bénéficiant des avantages concurrentiels liés, par exemple, à un label ou à une marque de protection de la vie privée. Certains de ces instruments peuvent être mis au point en tant que mécanismes propres au transfert ou dans le cadre d'outils plus généraux

[44] Voir l'article 46, paragraphe 2, points c) et d), et le considérant 109 du RGPD, qui précisent que des adaptations à des clauses types approuvées sont possibles tant qu'elles ne contredisent pas, directement ou indirectement, ces clauses types et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes physiques.

destinés à démontrer le respect de toutes les dispositions du RGPD, comme dans le cas d'un code de conduite approuvé.

La Commission collaborera avec les entreprises, la société civile et les autorités chargées de la protection des données en vue de tirer pleinement parti du potentiel que recèle la panoplie d'instruments du RGPD pour les transferts internationaux. Le dialogue en cours avec les parties prenantes dans le cadre de la mise en œuvre de la réforme permettra de recenser les domaines d'action prioritaires à cet égard. Il peut s'agir, notamment, de l'achèvement de travaux déjà entamés, par exemple en ce qui concerne l'établissement, en coopération avec le groupe de travail «article 29» (qui sera remplacé en 2018 par le comité européen de la protection des données), de CCT de sous-traitant à sous-traitant[45]. Il peut également s'agir de l'élaboration de nouvelles composantes de l'infrastructure européenne de conformité aux principes, grâce, par exemple, à la définition par la Commission d'exigences et de normes techniques pour la mise en place et le fonctionnement des mécanismes de certification, y compris pour les aspects relatifs aux transferts internationaux[46]. Certaines de ces actions peuvent être complétées par des travaux au niveau international, notamment avec les organisations qui ont mis au point des mécanismes de transfert similaires. Par exemple, il conviendrait de trouver des moyens de favoriser la convergence entre les REC en vertu du droit de l'Union et les règles transfrontalières de protection de la vie privée mises au point par la Coopération économique Asie-Pacifique (APEC)[47], en ce qui concerne tant les normes applicables que la procédure de demande dans le cadre de chaque système, ce qui devrait contribuer à promouvoir des normes élevées de protection des données au niveau mondial tout en réduisant les différences d'approche en matière de vie privée et de protection des données, aidant ainsi les opérateurs commerciaux à naviguer entre les différents systèmes et à élaborer des politiques qui soient conformes à ceux-ci.

La Commission entend:

- œuvrer avec les parties prenantes à la mise au point d'autres mécanismes de transfert de données à caractère personnel adaptés aux conditions ou aux besoins particuliers de certains secteurs, modèles commerciaux et/ou opérateurs.

3.3 Coopération internationale dans le domaine de la protection des données à caractère personnel

3.3.1. Promouvoir les normes de protection des données grâce aux enceintes et aux instruments multilatéraux

[45] À l'heure actuelle, aucune CCT de sous-traitant UE à sous-traitant non UE n'est en place.

[46] Article 43, paragraphes 8 et 9, du RGPD.

[47] Voir le référentiel commun APEC/UE de 2014 concernant la structure des règles d'entreprise contraignantes de l'UE et le système de règles transfrontalières de protection de la vie privée de l'APEC, qui compare les exigences de conformité et de certification des deux systèmes: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

Le cadre juridique de l'UE en matière de protection des données a souvent servi de point de référence pour l'élaboration de la législation de pays tiers dans ce domaine. L'UE continuera à dialoguer activement avec ses partenaires internationaux, au niveau bilatéral et multilatéral, afin de promouvoir la convergence par l'élaboration, au niveau mondial, de normes élevées et interopérables en matière de protection des données à caractère personnel. Cela contribue à accroître l'efficacité de la protection des droits des personnes, tout en réduisant les entraves à la circulation transfrontière des données, qui est un élément important du libre-échange.

En particulier, la Commission encourage l'adhésion des pays tiers à la convention 108 du Conseil de l'Europe et à son protocole additionnel[48]. Cette convention, qui est ouverte aux pays non membres du Conseil de l'Europe et a déjà été ratifiée par 50 pays, notamment des États d'Afrique et d'Amérique du Sud[49], est le seul instrument multilatéral contraignant dans le domaine de la protection des données. Elle est actuellement en cours de révision et la Commission encouragera activement l'adoption rapide du texte modernisé pour que l'UE y devienne partie. Elle reflétera les mêmes principes que ceux consacrés dans les nouvelles règles de l'UE en matière de protection des données, contribuant ainsi à la convergence vers un ensemble de normes élevées en matière de protection des données.

La réunion du G20 qui aura lieu en 2017 offrira à l'UE une occasion supplémentaire d'œuvrer pour une convergence autour du principe selon lequel des normes élevées de protection des données sont un élément essentiel de la poursuite de la mise en place d'une société de l'information mondiale capable de promouvoir l'innovation, la croissance et la prospérité sociale[50].

La Commission attend également avec intérêt de nouer le dialogue avec de nouveaux acteurs importants, tels que le rapporteur spécial des Nations unies sur le droit à la vie privée[51], et d'approfondir ses relations de travail avec des organisations régionales telles que l'APEC, afin de promouvoir, à l'échelle mondiale, une culture de respect des droits à la vie privée et à la protection des données à caractère personnel.

Dans le cadre de ses efforts visant plus largement à renforcer la sensibilisation à la protection de la vie privée et à relever le niveau des garanties en matière de protection des données au niveau international, la Commission européenne a approuvé, le 15 novembre 2016, au titre de l'instrument de partenariat, un projet visant à renforcer la coopération avec les pays partenaires dans ce domaine[52]. Ce projet consistera notamment à financer des activités telles que la formation et la sensibilisation. Pour sa part, dans le cadre de la mise en œuvre de la

---

48 Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 180) et protocole additionnel de 2001 à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE nº 181).

49 Maurice, le Sénégal et l'Uruguay ont ratifié la convention. En outre, le Cap-Vert, le Maroc et la Tunisie ont été invités à y adhérer.

50 Voir aussi la déclaration ministérielle de l'OCDE sur l'économie numérique: innovation, croissance et prospérité sociale («déclaration de Cancún»), 23 juin 2016.

51 Voir http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

52 Décision d'exécution C(2016)7198 de la Commission, approuvant la deuxième phase du programme d'action annuel 2016 (PAA 2016) de l'instrument de partenariat.

réforme, l'UE peut tirer profit de l'échange de bonnes pratiques et de l'expérience d'autres systèmes avec de nouveaux défis pour la protection de la vie privée et des solutions juridiques ou techniques émergentes, y compris en ce qui concerne le contrôle de l'application, les outils de conformité (par exemple, les mécanismes de certification, les analyses d'impact sur la vie privée) ou les protections pour certains ensembles de données (par exemple, les données relatives aux enfants).

3.3.2. Coopération en matière d'application de la loi

Le renforcement de la coopération avec les autorités des pays tiers compétentes en matière d'application et de contrôle du respect de la vie privée est de plus en plus nécessaire compte tenu de la dimension mondiale des entreprises multinationales qui traitent de grandes quantités de données à caractère personnel dans un grand nombre de pays. Souvent, les problèmes de non-conformité aux règles en matière de protection des données ou les violations de données touchent des personnes dans plusieurs juridictions simultanément. Dans ces cas, l'efficacité de la protection des personnes physiques pourrait être accrue grâce à une action commune. Dans le même temps, les opérateurs économiques tireraient avantage d'un environnement juridique plus clair si des outils communs d'interprétation et des pratiques communes d'application de la loi étaient élaborés au niveau mondial.

Dans le monde connecté et sans frontières des flux de données, il est donc temps d'intensifier la coopération entre les autorités chargées de l'application de la loi[53]. L'UE est prête à assumer sa part de responsabilité. Comme cela a été rappelé plus haut, le RGPD permet à la Commission d'élaborer des mécanismes de coopération internationale destinés à faciliter l'application effective de la législation en matière de protection des données, y compris au moyen d'accords d'assistance mutuelle. Dans ce contexte, il conviendrait d'explorer la possibilité de mettre en place un accord-cadre de coopération entre les autorités de protection des données de l'UE et les autorités chargées de l'application de la loi de certains pays tiers, en tirant parti de l'expérience acquise par la Commission dans d'autres domaines, tels que la concurrence et la protection des consommateurs.

[53] Parmi les réseaux existants figurent le Global Privacy Enforcement Network (GPEN), lancé en 2010 sous les auspices de l'OCDE. Il s'agit d'un réseau informel des autorités d'application des règles de protection de la vie privée, auquel participent les ADP de l'UE, chargé, entre autres, de la coopération en matière répressive, de l'échange de bonnes pratiques en matière de règlement des problèmes transfrontières et du soutien aux initiatives conjointes d'application de la loi et aux campagnes de sensibilisation. Il ne crée pas de nouvelles obligations juridiquement contraignantes entre les participants et se concentre essentiellement sur les moyens de faciliter la coopération dans l'application des lois régissant la protection de la vie privée dans le secteur privé. Voir https://privacyenforcement.net/.

La Commission entend:

- promouvoir l'adoption rapide du texte modernisé de la convention 108 du Conseil de l'Europe pour que l'UE y devienne partie et encourager l'adhésion de pays tiers;

- utiliser des enceintes multilatérales telles que les Nations unies, le G20 et l'APEC pour favoriser une culture mondiale du respect des droits en matière de protection des données;

- élaborer des mécanismes de coopération internationale avec les principaux partenaires internationaux afin de faciliter l'application effective de ces droits.

4. UNE COOPÉRATION PLUS EFFICACE DES AUTORITÉS RÉPRESSIVES AVEC DES GARANTIES SOLIDES EN MATIÈRE DE PROTECTION DES DONNÉES

Les échanges de données à caractère personnel font partie intégrante de la prévention et de la poursuite des infractions pénales, ainsi que des enquêtes les concernant. Dans un monde interconnecté où la criminalité s'arrête rarement aux frontières nationales, un échange rapide des données à caractère personnel est essentiel pour assurer le succès de la coopération des autorités répressives et pour lutter efficacement contre la criminalité. Ces échanges doivent reposer sur des garanties solides en matière de protection des données. Cela contribue également à l'instauration d'un climat de confiance entre les autorités répressives et au renforcement de la sécurité juridique lors de la collecte et/ou de l'échange d'informations.

Les règles relatives aux transferts internationaux figurant dans la directive «police» régissent les échanges de données entre les autorités répressives de l'UE et des pays tiers, ainsi que, dans certaines situations, les transferts de données des autorités répressives à d'autres entités. Cette directive introduit la possibilité d'établir des constats d'adéquation dans le domaine répressif. La Commission encouragera la possibilité d'établir de tels constats d'adéquation avec les pays tiers entrant en ligne de compte, plus particulièrement avec les pays avec lesquels une coopération étroite et rapide est requise dans la lutte contre la criminalité et le terrorisme, et lorsque d'importants échanges de données à caractère personnel existent déjà. Sur cette base, la Commission accordera la priorité aux discussions sur les décisions d'adéquation avec les pays tiers constituant des partenaires clés dans cet effort.

Par ailleurs, l'accord-cadre sur la protection des données entre l'UE et les États-Unis[54], conclu en décembre 2016, constitue un bon exemple de la manière dont la coopération en matière répressive avec un partenaire international important peut être renforcée en négociant un ensemble solide de garanties en matière de protection des données. En complétant automatiquement les instruments juridiques sur lesquels reposent actuellement les échanges

[54] 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 matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et judiciaire en matière pénale: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (l'«accord-cadre»).

de données (en particulier les accords bilatéraux au niveau tant de l'UE que des États membres), cet accord-cadre apporte des bénéfices immédiats et directs aux personnes physiques et renforce la coopération entre les autorités répressives en facilitant l'échange d'informations. En outre, en établissant une valeur de référence pour les futurs accords de transfert de données avec les États-Unis, cet accord-cadre supprime la nécessité de renégocier plusieurs fois les mêmes garanties. Il constitue le premier accord international bilatéral assorti d'un catalogue complet des droits et des obligations en matière de protection des données conformément à l'acquis de l'UE et peut, dès lors, servir de base pour négocier des accords similaires avec des pays tiers non seulement dans le domaine de la coopération judiciaire et policière, mais aussi dans d'autres domaines de l'application de la loi par les autorités publiques (par exemple, la politique de concurrence ou la protection des consommateurs). Seraient couverts à la fois les échanges entre pouvoirs publics et les transferts de données entre entreprises privées et autorités répressives. Il pourrait également faciliter la conclusion, par l'Union, d'accords concernant les échanges de données entre les agences de l'UE concernées (notamment Europol et Eurojust) et des pays tiers[55]. La Commission explorera donc la possibilité de conclure des accords-cadres similaires avec ses grands partenaires en matière répressive.

En outre, la directive «police» prévoit la possibilité pour les autorités répressives de l'UE, sous réserve de garanties strictes et dans des circonstances spécifiques, de demander des informations directement auprès d'une entreprise privée dans un pays tiers et de transmettre des informations à caractère personnel (généralement un nom ou une adresse IP) dans cette demande[56]. Le RGPD aborde, quant à lui, spécifiquement les cas où des entités privées au sein de l'UE transmettent des données à caractère personnel aux autorités répressives d'un pays tiers à la suite d'une demande: ces transferts en dehors de l'UE ne sont admis qu'à certaines conditions, par exemple sur la base d'un accord international ou lorsque la divulgation est nécessaire pour un motif important d'intérêt général reconnu par le droit de l'Union ou la législation d'un État membre[57].

Cette coopération, qui est devenue un élément central de la réussite des enquêtes et des poursuites pour des actes de criminalité et de terrorisme, est mise en lumière dans les conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace. Le Conseil a invité la Commission à prendre des mesures concrètes fondées sur une approche commune de l'UE, à renforcer la coopération avec les fournisseurs de services, à rendre l'entraide judiciaire plus efficace et à proposer des solutions aux problèmes de la détermination et de l'application de la compétence dans le cyberespace[58]. Ces actions couvrent tant les échanges entre les autorités répressives et les fournisseurs de services établis dans l'UE que les

[55] La conclusion d'accords opérationnels avec Europol et Eurojust a également été un paramètre de référence dans les dialogues sur la libéralisation du régime des visas avec certains pays tiers, notamment dans le cadre du dialogue en cours avec la Turquie.

[56] Voir l'article 39 et le considérant 73 de la directive «police».

[57] Voir l'article 48 et le considérant 115 du RGPD.

[58] Conclusions du Conseil de l'Union européenne sur l'amélioration de la justice pénale dans le cyberespace, 9 juin 2016: http://data.consilium.europa.eu/doc/document/ST-10007-2016-INIT/fr/pdf. La Commission a été chargée de présenter au Conseil d'ici juin 2017 les résultats escomptés sur ces questions, à la suite de son rapport sur l'état d'avancement soumis au Conseil en décembre 2016.

échanges avec les autorités et les entreprises de pays tiers. La Commission présentera différentes options pour l'accès aux preuves électroniques en juin 2017, en tenant compte de la nécessité d'une coopération rapide et fiable, reposant sur les normes solides en matière de protection des données prévues dans la directive «police» et le RGPD tant pour les situations internes à l'Union que pour les transferts internationaux.

Enfin, conformément à la nouvelle base juridique applicable à Europol, la Commission évaluera les dispositions contenues dans ces accords de coopération opérationnelle entre Europol et des tiers, conclus en vertu de la décision 2009/371/JAI du Conseil, y compris leurs dispositions en matière de protection des données[59]. En outre, comme indiqué dans le programme européen en matière de sécurité de 2015, l'approche qu'adoptera l'Union en matière d'échange de données PNR avec des pays tiers tiendra compte de la nécessité d'appliquer des normes cohérentes et des protections propres aux droits fondamentaux. La Commission s'attachera à trouver des solutions juridiquement solides et durables en matière d'échange de données des dossiers passagers (données PNR) avec les pays tiers, et envisagera notamment la possibilité d'élaborer un modèle d'accord PNR définissant les exigences auxquelles un pays tiers doit satisfaire pour recevoir des données PNR de l'UE. Toute future politique dans ce domaine dépendra toutefois, notamment, de l'avis que rendra la Cour de justice de l'Union européenne sur l'accord PNR envisagé entre l'UE et le Canada[60].

UNE COOPÉRATION PLUS EFFICACE DES AUTORITÉS RÉPRESSIVES AVEC DES GARANTIES SOLIDES EN MATIÈRE DE PROTECTION DES DONNÉES

La Commission entend:

- favoriser la possibilité d'adopter des décisions d'adéquation en vertu de la directive «police» avec les pays tiers entrant en ligne de compte;

- promouvoir la négociation d'accords dans le domaine répressif avec d'importants partenaires internationaux sur le modèle fourni par l'accord-cadre avec les États-Unis;

- donner suite aux conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace en vue de faciliter l'échange transfrontière de preuves électroniques dans le respect des règles en matière de protection des données.

[59] Voir l'article 25, paragraphe 4, du règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, JO L 135 du 24.5.2016, p. 53. La Commission est tenue de présenter un rapport d'évaluation au plus tard le 14 juin 2021 sur les accords de coopération conclus par Europol avant le 1er mai 2017.

[60] Avis de la Cour de justice sur le projet d'accord PNR UE-Canada de 2014, soumis à la Cour par le Parlement européen (avis 1/15). La Cour a été invitée à examiner la compatibilité du projet d'accord avec la charte des droits fondamentaux de l'UE.

5. CONCLUSION

La protection et l'échange des données à caractère personnel ne sont pas incompatibles. Un système solide de protection des données facilite les flux de données en renforçant la confiance des consommateurs envers les entreprises qui se soucient de la manière dont elles traitent les données à caractère personnel de leurs clients. Des normes élevées en matière de protection des données deviennent donc un avantage dans l'économie numérique mondiale. Il en va de même pour la coopération des autorités répressives: les garanties en matière de protection de la vie privée font partie intégrante de l'échange rapide et efficace d'informations dans le cadre de la lutte contre la criminalité, sur la base de la confiance mutuelle et de la sécurité juridique.

Après avoir mené à bien la réforme de ses règles en matière de protection des données, l'UE devrait entamer un dialogue avec les pays tiers sur cette question. Elle devrait s'efforcer de rechercher une plus grande convergence des principes en matière de protection des données au niveau international, sur le plan tant bilatéral que multilatéral, et ce dans l'intérêt et au bénéfice des citoyens et des entreprises. Le nouveau cadre législatif en matière de protection des données confère à l'UE les outils nécessaires et appropriés pour réaliser ces objectifs. Sur la base de l'approche stratégique présentée dans la présente communication, la Commission coopérera activement avec des pays tiers clés pour étudier la possibilité d'adopter des constats d'adéquation, en commençant par le Japon et la Corée en 2017, dans le but d'encourager la convergence réglementaire vers les normes de l'UE et de faciliter les relations commerciales. Dans le même temps, l'UE tirera pleinement parti de l'éventail des autres outils de transfert afin de protéger les droits à la protection des données et de soutenir les opérateurs économiques lorsque des données sont transférées vers des pays dont le droit interne ne garantit pas un niveau adéquat de protection des données. Ces outils devraient également être utilisés pour continuer à faciliter la coopération entre les autorités de contrôle et les autorités répressives de l'UE, d'une part, et leurs partenaires internationaux, d'autre part. La Commission veillera à la cohérence de la dimension interne et externe de la politique européenne en matière de protection des données et agira en faveur d'une protection forte des données au niveau international afin d'améliorer la coopération entre les autorités répressives, de contribuer au libre-échange et d'élaborer des normes élevées en matière de protection des données à caractère personnel à l'échelle mondiale.