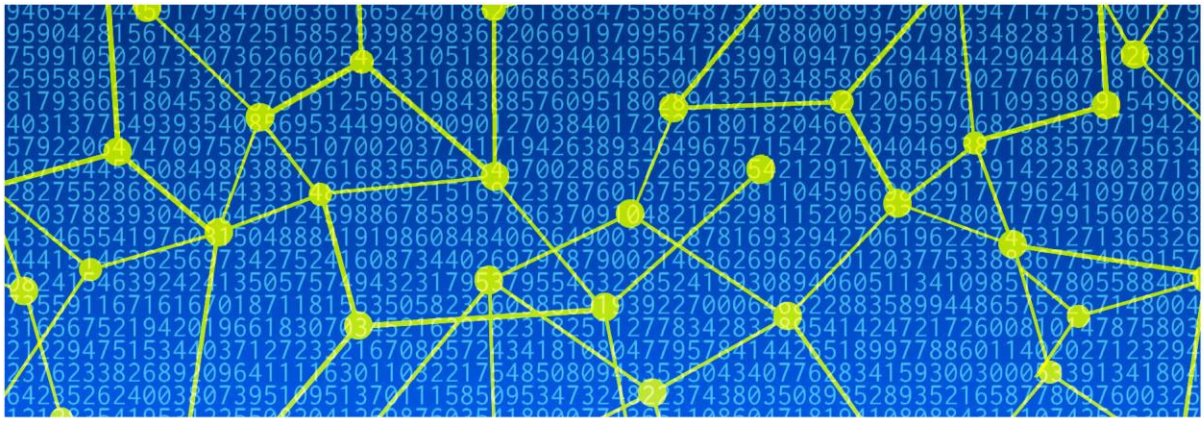

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 2/2019

Avis du CEPD sur le mandat de négociation d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques

EDPS

2 avril 2019

Le Contrôleur européen de la protection des données (ci-après le «CEPD») est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[...] [e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union», et en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». En vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec pour mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'Union européenne sur l'application cohérente et logique des principes de protection des données de l'Union européenne lors de la négociation d'accords dans le secteur répressif, conformément à l'action n° 5 de la stratégie du CEPD: «Intégrer la protection des données dans les politiques internationales». Cet avis s'appuie sur l'obligation générale exigeant que les accords internationaux conclus par l'Union soient conformes aux dispositions du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE») et respectent les droits fondamentaux qui forment le noyau du droit de l'Union. En particulier, il convient de veiller à ce que l'article 8 de la charte des droits fondamentaux de l'Union européenne ainsi que l'article 16 du TFUE soient respectés.

Synthèse

Le 5 février 2019, la Commission européenne a émis une recommandation de décision du Conseil autorisant l'ouverture de négociations en vue de conclure un accord international avec les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques. L'annexe de la recommandation définit les directives du Conseil pour la négociation de cet accord. La proposition d'accord aurait pour objet de traiter, au moyen de règles communes, la question juridique de l'accès aux données relatives ou non relatives au contenu détenues par des fournisseurs de services dans l'Union européenne et aux États-Unis d'Amérique.

Le CEPD salue et soutient l'objectif de la Commission de conclure avec les États-Unis d'Amérique un accord sur l'accès transfrontière aux preuves électroniques, qui garantirait ainsi un degré élevé de protection des données à caractère personnel transférées entre l'Union européenne et les États-Unis à des fins répressives, et apprécie son engagement en faveur de l'introduction de garanties suffisantes. Comme le préconise le CEPD depuis longtemps, l'Union doit conclure avec des pays tiers des accords viables concernant le partage de données à caractère personnel à des fins répressives, qui soient pleinement compatibles avec la charte des droits fondamentaux. Même lorsqu'elles enquêtent sur des affaires internes, les autorités répressives rencontrent de plus en plus souvent des «questions transfrontières», tout simplement parce qu'un fournisseur de services étranger a été utilisé et que les informations sont stockées sous forme électronique dans un pays tiers. En pratique, il s'agit souvent de fournisseurs de services dont le siège social est établi aux États-Unis d'Amérique en raison de la position dominante de ces derniers sur les marchés mondiaux. Le volume croissant de demandes de preuves électroniques et le caractère volatil des informations numériques met à mal les modèles de coopération existants, tels que les traités d'entraide judiciaire. Le CEPD entend bien que les autorités sont engagées dans une course contre la montre lorsqu'il s'agit d'obtenir des données pour leurs enquêtes, et soutient les efforts en vue de concevoir de nouveaux modèles de coopération, y compris dans le contexte de la coopération avec des pays tiers.

Le présent avis vise à fournir des recommandations constructives et objectives alors que le Conseil doit émettre ses directives avant que cette tâche délicate ne commence. Il s'appuie sur la jurisprudence de la Cour de justice de l'Union européenne de ces dernières années, qui confirme les principes relatifs à la protection des données, y compris la loyauté, l'exactitude et la pertinence des informations, la supervision indépendante et les droits individuels des personnes. De tels principes s'imposent tant aux organismes publics qu'aux entreprises privées et sont particulièrement importants compte tenu du caractère sensible des données nécessaires à la poursuite des enquêtes pénales.

Dans ce contexte, le CEPD souhaite formuler les observations suivantes:
- il salue le fait que la recommandation inclut déjà d'importantes garanties relatives à la protection des données, notamment la nécessité de rendre l'accord-cadre applicable en s'y référant, et soutient la nécessité de le compléter par des garanties supplémentaires, comme le propose la Commission;
- compte tenu des risques spécifiques existant dans le contexte d'une coopération directe entre les fournisseurs de services et les autorités judiciaires, il propose que l'autre partie à l'accord fasse participer une autorité judiciaire;
- il recommande d'ajouter l'article 16 du TFUE en tant que base juridique matérielle.

En outre, l'avis émet des recommandations supplémentaires relatives à des améliorations et des éclaircissements possibles à apporter aux directives de négociation. Le CEPD se tient à la disposition des institutions pour tout conseil complémentaire au cours des négociations et avant la finalisation du futur accord entre les États-Unis d'Amérique et l'Union européenne.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le 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)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[2], et en particulier l'article 42, paragraphe 1, l'article 57, paragraphe 1, point g), et l'article 58, paragraphe 3, point c), de celui-ci,

vu la 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[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. Le 17 avril 2018, la Commission a présenté conjointement deux propositions législatives: une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[4] (ci-après la «proposition relative aux preuves électroniques»), ainsi qu'une proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale[5]. Bien que les travaux préparatoires se poursuivent au Parlement européen, le Conseil de l'Union européenne (ci-après le «Conseil») est parvenu à adopter une orientation générale sur ces deux propositions[6].

2. Le 5 février 2019, la Commission a adopté deux recommandations relatives aux décisions du Conseil: une recommandation d'autoriser l'ouverture de négociations en vue d'un accord international entre l'Union européenne (ci-après l' «Union» ou l'«UE») et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale[7] (ci-après la «recommandation»), ainsi qu'une recommandation d'autoriser la Commission à participer aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STCE nº 185)[8]. L'annexe de la recommandation (ci-après l'«annexe») est de la plus haute importance puisqu'elle établit les directives de négociation recommandées à la Commission par le Conseil en vue de conclure l'accord au nom de l'Union européenne. La seconde recommandation fait l'objet d'un avis distinct du CEPD[9]. Le CEPD estime néanmoins que les deux négociations, celle engagée avec les États-Unis d'Amérique et celle au sein du Conseil de l'Europe, sont étroitement liées.

3. La recommandation a été adoptée conformément à la procédure établie à l'article 218 du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE») relativement aux accords conclus entre l'Union et les pays tiers. Par ladite recommandation, la Commission vise à obtenir du Conseil l'autorisation de négocier au nom de l'Union et à engager les négociations avec les États-Unis d'Amérique, selon les directives de négociation annexées à la recommandation. Une fois les négociations terminées, et en vue de conclure cet accord, le Parlement européen devra approuver le texte de l'accord négocié, puis le Conseil adoptera une décision visant à déclarer cet accord conclu formellement. Le CEPD s'attend à être consulté sur le texte du projet d'accord en temps voulu, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725.

4. Le CEPD se félicite d'avoir été consulté par la Commission européenne à la suite de l'adoption de la recommandation, ainsi que par la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen. Le CEPD salue également la référence faite à son avis dans le considérant 4 de la recommandation. Il souhaite souligner que le présent avis est délivré sans préjudice des commentaires additionnels que le CEPD pourrait émettre sur la base d'informations supplémentaires disponibles ultérieurement.

2. OBJECTIFS DE L'ACCORD

5. L'initiative de la Commission a pour objet de traiter la question juridique spécifique de l'accès aux données relatives ou non relatives au contenu détenues par des fournisseurs de services dans l'Union européenne et aux États-Unis d'Amérique, au moyen de règles communes établies dans un accord international. Un tel accord viendrait ainsi compléter la proposition relative aux preuves électroniques en remédiant aux conflits de lois entre l'Union et les États-Unis d'Amérique, et, dans la mesure où les plus grands fournisseurs de services ont leur siège aux États-Unis d'Amérique, rendrait ladite proposition plus efficace.

6. Les États-Unis d'Amérique ont conclu avec la plupart des États membres des traités d'entraide judiciaire bilatéraux en vue d'échanger des preuves en matière pénale. Le traité d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique[10], signé en 2003 et entré en vigueur en 2010, vient compléter ces accords bilatéraux. La Commission considère qu'il est nécessaire de développer des voies alternatives à la coopération judiciaire entre l'Union et les États-Unis d'Amérique et de permettre une coopération directe entre les autorités judiciaires et les fournisseurs de services dans le cadre des relations transatlantiques.

7. Une coopération directe avec les fournisseurs de services américains existe déjà en pratique, dans une certaine mesure. La législation américaine permet aux fournisseurs de services établis aux États-Unis d'Amérique de coopérer directement avec les autorités publiques étrangères[11]. Cette coopération ne concerne que les données non relatives au contenu et se fait sur une base volontaire du point de vue de la législation américaine[12]. Les entreprises américaines ont adopté leurs propres politiques en réponse aux demandes émanant d'autorités étrangères ou se prononcent au cas par cas, en conséquence de quoi les demandes émises auprès de fournisseurs de services américains ne sont souvent pas satisfaites[13]. En outre, cette pratique crée une certaine insécurité juridique. Le *Stored Communications Act* (loi américaine sur les communications stockées) interdit la divulgation aux autorités étrangères de données relatives au contenu. En application du *Clarifying Lawful Overseas Use of Data (CLOUD) Act* (loi américaine visant à clarifier l'utilisation légale des données à l'étranger)[14], les fournisseurs de services américains pourraient accéder aux demandes de

données relatives au contenu émanant de gouvernements étrangers répondant à certains critères et ayant conclu un accord exécutif avec les États-Unis d'Amérique[15].

8. Selon la Commission, un accord entre l'Union et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques complèterait la proposition relative aux preuves électroniques, qui pourrait entraîner des obligations contradictoires découlant des législations des pays tiers, et aborder les questions juridiques auxquelles les autorités répressives sont confrontées lorsqu'elles cherchent à accéder à des données relatives et non relatives au contenu détenues par des fournisseurs de services dans l'Union ou aux États-Unis d'Amérique[16]. L'accord envisagé poursuivrait les trois objectifs principaux détaillés dans les paragraphes 1, 2 et 3 des directives de négociation énoncées dans l'annexe:

   1) fixer des règles communes et prévenir les conflits de lois pour les injonctions relatives à l'obtention de preuves électroniques sous la forme de données relatives ou non relatives au contenu, adressées par les autorités judiciaires aux fournisseurs de services dans un contexte transfrontière, afin d'améliorer la sécurité juridique;
   2) permettre les transferts de preuves électroniques entre les acteurs précités lorsqu'ils coopèrent directement;
   3) garantir le respect des libertés et droits fondamentaux et des principes généraux du droit de l'Union, notamment le droit au respect de la vie privée et à la protection des données.

3. RECOMMANDATIONS PRINCIPALES

9. Le CEPD soutient ces efforts visant à trouver des approches innovantes afin d'obtenir l'accès transfrontière aux preuves électroniques. Il soutient l'analyse de la Commission selon laquelle *«il est dans l'intérêt de l'Union européenne de conclure un accord global avec les États-Unis d'Amérique, tant pour protéger les droits et valeurs européens, tels que le respect de la vie privée et la protection des données à caractère personnel, que pour préserver ses propres intérêts en matière de sécurité»*[17]. Un accord entre l'Union et les États-Unis d'Amérique permettrait de mieux préserver le niveau de protection garanti par le cadre européen en matière de protection des données, et de garantir un niveau cohérent de protection dans l'ensemble de l'Union européenne, plutôt qu'une série d'accord distincts conclus bilatéralement par les États membres.

3.1. Normes concernant les transferts internationaux de données et le respect des droits fondamentaux

10. Le second objectif de l'accord international envisagé, énoncé dans les directives de négociation, dispose que cet accord prévoira *«un transfert de preuves électroniques, direct et sur une base réciproque, d'un fournisseur de services à une autorité requérante»*[18].

11. En vertu de l'article 216, paragraphe 2, du TFUE, les accords internationaux auxquels l'Union est partie, tels que l'accord envisagé, «*lient les institutions de l'Union et les États membres*». En outre, conformément à une jurisprudence constante de la Cour de justice de l'Union européenne (ci-après la «CJUE»), les accords internationaux «*forment partie intégrante de [l'ordre juridique européen]*» dès leur entrée en vigueur[19].

12. En ce qui concerne les accords internationaux conclus par l'Union, la CJUE a conclu que «*les obligations qu'impose un accord international ne sauraient avoir pour effet de porter atteinte aux principes constitutionnels du traité CE, au nombre desquels figure le principe*

selon lequel tous les actes [de l'Union] doivent respecter les droits fondamentaux, ce respect constituant une condition de leur légalité qu'il incombe à la Cour de contrôler dans le cadre du système complet de voies de recours qu'établit ce traité»[20]. L'analyse ultérieure prend pour point de départ l'exigence incombant aux accords internationaux de se conformer au système de l'Union en matière de protection des droits fondamentaux. Non seulement la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») garantit le respect de la vie privée et familiale (article 7), mais elle a également élevé la protection des données au rang de droit fondamental dans le droit de l'Union (article 8).

13. La CJUE a pris en considération les normes applicables du droit de l'Union au regard des accords internationaux prévoyant des transferts de données à caractère personnel. En juillet 2017, dans son avis 1/15[21] concernant l'accord international sur le transfert de données des dossiers passagers au Canada (*Passenger Name Records*, ci-après les «PNR»), la CJUE précise les conditions dans lesquelles un accord international peut constituer une base légale pour le transfert de données à caractère personnel. La CJUE a estimé qu'*«un transfert de données à caractère personnel depuis l'Union vers un pays tiers ne peut avoir lieu que si ce pays assure un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union»*[22]. Il résulte de l'avis 1/15 que le niveau de protection découlant des accords envisagés avec les États-Unis d'Amérique sur l'échange de données à caractère personnel entre les autorités nationales compétentes et les fournisseurs de services à des fins répressives devrait, de la même façon (que l'accord entre l'Union européenne et le Canada sur le transfert des données PNR), être essentiellement équivalent au niveau de protection offert par le droit de l'Union.

14. Dans ce contexte, il convient d'attirer l'attention sur l'article 35, paragraphe 1, de la directive en matière de protection des données dans le domaine répressif[23], qui détaille les conditions spécifiques dans lesquelles l'autorité répressive d'un État membre peut légalement transférer des données à des destinataires établis dans des pays tiers; y est inscrit notamment le principe selon lequel, en règle générale, le destinataire de tels transferts doit être une autorité compétente du pays tiers en matière de «prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces». Les transferts par les autorités répressives des États membres à d'autres destinataires, y compris des parties privées établies dans des pays tiers, sont autorisés uniquement à titre dérogatoire au titre de l'article 39 de la directive en matière de protection des données dans le domaine répressif[24], et uniquement si certaines conditions supplémentaires[25] sont remplies. Parmi ces conditions particulières figure, notamment, l'obligation d'informer l'autorité chargée de la protection des données compétente dans leur État membre, et l'obligation de documenter le transfert[26]. Le CEPD considère que le futur accord entre l'Union européenne et les États-Unis d'Amérique devrait au moins inclure des conditions supplémentaires inspirées de l'article 39 de la directive en matière de protection des données dans le domaine répressif, afin de ne pas réduire le niveau de protection des données établi par ladite directive.

3.2. Base juridique de la décision du Conseil

15. L'exposé des motifs de la recommandation dispose que «*le Conseil autorise l'ouverture de négociations, adopte des directives de négociation et autorise la signature et la conclusion de l'accord conformément à l'article 218, paragraphes 3 et 4, du traité sur le fonctionnement de l'Union européenne*»[27]. Il est également fait référence à l'article 218,

paragraphes 3 et 4, du TFUE dans le préambule du projet de décision du Conseil. Toutefois, le préambule ne fait référence à aucune base juridique matérielle pour cet acte juridique.

16. Conformément à l'article 296, paragraphe 2, du TFUE et à la jurisprudence constante de la CJUE[28], le CEPD s'interroge sur le fait que les visas cités dans le préambule de la décision du Conseil font certes référence aux bases juridiques procédurales appropriées, mais ne font pas de la même manière référence aux bases juridiques matérielles pertinentes.

17. **Le CEPD recommande que les visas cités dans le préambule de la décision du Conseil fassent non seulement référence à la base juridique procédurale adéquate mais également à la base juridique matérielle pertinente, notamment à l'article 16 du TFUE.** Il s'ensuit déjà de la section 1 de l'annexe portant sur les directives de négociation que la Commission devrait poursuivre plusieurs objectifs simultanément lors des négociations en vue de l'accord envisagé, parmi lesquels prévoir le transfert de données à caractère personnel et garantir le respect des droits fondamentaux inscrits dans la charte, notamment le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. De cette manière, l'accord envisagé serait directement en rapport avec les objectifs visés par l'article 16 du TFUE. Le CEPD rappelle que, dans un contexte répressif similaire, la CJUE a conclu que «*la décision du Conseil relative à la conclusion de l'accord envisagé [entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers] doit être fondée conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), TFUE*»[29].

3.3. Garanties contenues dans l'accord-cadre et garanties supplémentaires

18. Les directives de négociation contenues dans l'annexe disposent que *«[l]'accord devrait rendre applicable, en s'y référant, l'accord UE – États-Unis sur la protection des données et le respect de la vie privée, également connu sous le nom d'"accord-cadre"»*[30]. L'accord-cadre[31] est entré en vigueur le 1er février 2017 et établit un cadre pour la protection des données à caractère personnel échangées entre l'Union européenne et les États-Unis d'Amérique à des fins répressives[32]. L'accord-cadre ne constitue pas une base juridique pour les transferts de données à caractère personnel; en outre, une base juridique adéquate pour les transferts aux États-Unis d'Amérique est toujours nécessaire. Le droit de l'Union requiert toujours une base légale pour le transfert de données à caractère personnel effectué en réponse à une injonction relative à l'obtention de preuves électroniques.

19. **Le CEPD salue le fait que l'accord-cadre, qu'il a activement soutenu, s'applique par référence et soit inclus dans le mandat de négociation**. Dans le même temps, le CEPD rappelle que, dans son avis 1/2016 relatif à l'accord-cadre[33], il a préconisé des améliorations essentielles et a insisté sur la nécessité de renforcer plusieurs garanties. **Dans la mesure où lesdits problèmes n'ont pas été résolus dans le texte final de l'accord-cadre, le CEPD estime que les améliorations nécessaires** (abordées dans les sections ci-dessous[34]) **devraient être incluses dans les directives de négociation elles-mêmes.**

20. En règle générale, l'accord-cadre confère un **niveau de garanties minimal** aux transferts de données à caractère personnel aux États-Unis d'Amérique à des fins répressives. Tout en n'affaiblissant pas de telles garanties, l'accord envisagé devrait augmenter le niveau de protection des données, en tenant compte des spécificités de l'accord envisagé et des risques existant pour les droits et les libertés des personnes concernées. Par conséquent, le CEPD salue le fait que le paragraphe 15 du mandat de négociation envisage de telles garanties supplémentaires et dispose que *«[l]'accord devrait compléter l'accord-cadre par des*

garanties supplémentaires tenant compte du niveau de sensibilité des catégories de données concernées et des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités».

21. À cet égard, le CEPD rappelle que, pour respecter la condition de proportionnalité inscrite à l'article 52, paragraphe 1, de la charte, les avantages résultant des mesures ne doivent pas être contrebalancés par les inconvénients causés par de telles mesures au regard de l'exercice des droits fondamentaux[35]. Ils devraient établir un juste équilibre entre la nécessité d'accélérer la procédure en vue de recueillir et d'obtenir des preuves électroniques afin de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière, d'une part, et la protection efficace des données à caractère personnel et des autres droits fondamentaux des personnes concernées, d'autre part. **Le CEPD salue l'attention déjà portée à la protection de la vie privée et des données dans l'ensemble des directives de négociation incluses dans l'annexe, et soutient l'affirmation selon laquelle l'accord envisagé «*devrait être subordonné à la mise en place de solides mécanismes de protection des droits fondamentaux*»[36].** Il remarque que les paragraphes 16 et 17 des directives de négociation énumèrent une liste non exhaustive de garanties supplémentaires à inclure dans l'accord. **Il recommande de remplacer le mot «*notamment*» dans les paragraphes 16 et 17 par «à tout le moins» afin de mieux véhiculer le caractère indispensable de ces garanties.**

22. **En outre, compte tenu de l'incidence de l'accord envisagé sur les droits fondamentaux, le CEPD considère qu'au-delà des garanties envisagées dans les directives de négociation, certaines garanties supplémentaires** (qu'il abordera individuellement dans les sections ci-dessous[37]) **devraient être incluses afin de s'assurer que l'accord final respecte l'exigence de proportionnalité.**

23. Enfin, le CEPD rappelle que **toutes les garanties énoncées dans l'accord envisagé doivent être non seulement explicites mais également efficaces afin de respecter pleinement le droit primaire de l'Union européenne et d'être conformes à l'avis 1/15 de*la CJUE[38].**

3.4. Participation des autorités judiciaires de l'autre partie à l'accord

24. Les directives de négociation donnent clairement des instructions[39] en vue d'établir un modèle de coopération directe entre les autorités judiciaires et les fournisseurs de services; ce modèle est similaire au modèle envisagé dans la proposition relative aux preuves électroniques, avec pour distinction importante le fait qu'une telle coopération directe est envisagée entre les autorités d'un pays tiers - les États-Unis d'Amérique - et des fournisseurs de services situés dans l'Union européenne (et inversement). Le CEPD fait remarquer que de telles directives ne mentionnent pas une participation systématique des autorités judiciaires compétentes de l'autre partie lors de l'émission des injonctions. Le paragraphe 16, point (c), dispose que *«la divulgation des données à d'autres autorités américaines non liées par l'accord-cadre et l'utilisation de ces données par lesdites autorités font l'objet d'une notification à, et d'une autorisation préalable de, l'autorité judiciaire compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté»*. Il est difficile de déterminer si cette exigence de notification et d'autorisation préalable fait référence à toutes les injonctions émises par les autorités américaines compétentes non liées par l'accord-cadre, ou si elle fait référence à la communication de données par les autorités américaines liées par l'accord-cadre à d'autres autorités américaines non liées par celui-ci. **Le CEPD recommande de clarifier le paragraphe 16, point c)**.

25. Selon l'approche traditionnelle en matière d'accès transfrontière aux preuves électroniques, il incombe prioritairement à l'État d'exécution de garantir le contrôle de motifs de refus limités. Bien que le CEPD, comme il a été précisé ci-dessus, reconnaisse la nécessité de déterminer des approches alternatives aux fins de collecter des preuves dans un contexte transfrontière, la nécessité de garanties effectives des droits fondamentaux des personnes concernées demeure de la plus haute importance. Il importe de tenir compte du fait que les lois applicables dans les États membres de l'Union et aux États-Unis d'Amérique - notamment celles portant sur la recevabilité des preuves collectées dans un autre pays et sur ce qui constitue une infraction pénale - peuvent diverger.

26. En outre, les entités privées peuvent ne pas être équipées pour réaliser l'évaluation requise de manière efficace. Il est primordial de garder à l'esprit que les fournisseurs de services, bien qu'ils soient les destinataires des injonctions, ne sont pas ceux dont les droits à la vie privée et à la protection des données à caractère personnel sont limités par lesdites injonctions. Pourtant, les conditions d'émission de l'injonction ne sont pas harmonisées sur le fond au niveau international, et il peut exister d'importantes objections quant à la reconnaissance et aux modalités d'exécution d'une telle injonction[40]. Les États membres ont l'obligation légale de respecter les droits fondamentaux lors de la mise en œuvre du droit de l'Union[41]. À cet égard, dans le contexte des négociations relatives à la directive concernant la décision d'enquête européenne, l'Agence des droits fondamentaux a rappelé qu'«*une incapacité à garantir le respect adéquat des droits fondamentaux dans le cadre de l'exécution d'une décision d'enquête européenne engage la responsabilité de l'État d'exécution en vertu d'instruments tels que la Convention européenne des droits de l'homme*»[42].

27. Le CEPD souligne que le Conseil a adopté une orientation générale[43] concernant la proposition relative aux preuves électroniques en décembre 2018, qui introduit une notification aux autorités compétentes des États d'exécution membres de l'Union des injonctions demandant la production des données de contenu. Une telle notification doit être réalisée en même temps que les injonctions sont envoyées aux fournisseurs de services afin de donner la possibilité aux autorités notifiées de soulever certaines objections. Plusieurs États membres ont demandé que l'État membre où se situe le fournisseur de services participe davantage, au-delà de la notification introduite par l'orientation générale, et que celle-ci couvre également les données non relatives au contenu[44]. En outre, le comité européen de la protection des données, qui a émis un avis concernant la proposition relative aux preuves électroniques, n'a vu aucune justification au fait d'adresser des injonctions à produire des données relatives au contenu aux fournisseurs de services *«sans la participation au moins des autorités compétentes de l'État membre dans lequel se trouve la personne concernée»*[45].

28. En outre, même dans le contexte de l'Union européenne, le comité européen de la protection des données a exprimé, dans son avis portant sur la proposition relative aux preuves électroniques, «*ses préoccupations quant à la suppression de tout double contrôle de l'injonction transmise par l'autorité compétente destinataire par rapport aux autres instruments*»[46]. Le **CEPD estime que, dans ce contexte, la protection effective des droits fondamentaux requiert un niveau de participation des autorités publiques de la partie requise à l'accord envisagé. Il recommande par conséquent d'inclure dans les directives de négociation, en tant que garantie spécifique, l'obligation pour les autorités compétentes de l'Union et des États-Unis d'Amérique de faire participer**

systématiquement et aussi tôt que possible les autorités judiciaires désignées par l'autre partie au processus de collecte de preuves électroniques, afin de donner à ces autorités la possibilité de contrôler effectivement la conformité de l'injonction aux exigences en matière de droits fondamentaux, d'une part, et d'éventuellement soulever des motifs de refus, sur la base d'informations suffisantes et dans des délais raisonnables, d'autre part. Du point de vue de l'Union européenne, une telle participation des autorités judiciaires de l'Union serait davantage conforme aux dispositions de l'article 82, paragraphe 1, du TFUE (si une telle base juridique est incluse parmi les bases juridiques matérielles de la décision du Conseil).

4. RECOMMANDATIONS SUPPLÉMENTAIRES

29. Le CEPD souhaite insister sur l'importance de prévoir des garanties concrètes, spécifiques et efficaces. Compte tenu du contexte répressif et des risques potentiels que ces transferts de données pourraient présenter pour les personnes concernées, les garanties prévues dans ces accords internationaux avec les pays tiers devraient prévoir et atténuer ces risques de manière satisfaisante.

4.1. Caractère obligatoire de l'accord

30. Les directives de négociation précisent que l'accord envisagé devrait *«prévaloir sur la convention sur la cybercriminalité du Conseil de l'Europe et sur tout accord ou arrangement conclu à l'issue des négociations concernant le deuxième protocole additionnel»*. Toutefois, elles ne précisent pas si le *CLOUD Act* - qui a une portée clairement extraterritoriale - pourrait encore être utilisé par les autorités répressives américaines pour émettre des ordonnances prescrivant la divulgation de données aux entreprises de l'Union, si un accord sur l'accès transfrontière aux preuves électroniques était conclu entre l'Union et les États-Unis d'Amérique.

31. L'exposé des motifs dispose qu'*«il est dans l'intérêt tant de l'Union européenne que des États-Unis d'Amérique de conclure un accord global, car celui-ci offrirait une sécurité juridique aux autorités judiciaires et répressives des deux parties et éviterait aux fournisseurs de services d'être confrontés à des obligations juridiques contradictoires»*[47]. **Pour atteindre efficacement ces objectifs, le CEPD recommande de clarifier, dans les directives de négociation, le caractère obligatoire[48] de l'accord envisagé dans les relations bilatérales entre l'Union européenne et les États-Unis d'Amérique**.

32. En outre, les traités et les accords exécutifs conclus par les États-Unis d'Amérique pourraient ne pas avoir d'effet d'exécution directe puisqu'une législation d'application est nécessaire pour rendre leurs dispositions exécutoires aux États-Unis. Dès lors, **le CEPD recommande d'indiquer explicitement que l'accord envisagé doit être un accord d'exécution directe du point de vue du droit américain**.

4.2. Transferts ultérieurs

33. Le paragraphe 16, point d), des directives de négociation dispose que des *«transferts ultérieurs vers d'autres pays tiers ne peuvent se faire qu'aux autorités répressives [...] et devraient faire l'objet d'une notification à, et d'une autorisation préalable de, l'autorité judiciaire compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté»*. La CEPD salue ces exigences en matière de transferts ultérieurs,

semblables à celles établies à l'article 35 de la directive en matière de protection des données dans le domaine répressif[49]. Toutefois, **le CEPD considère qu'il conviendrait d'ajouter une condition supplémentaire aux transferts ultérieurs en s'assurant que la seconde autorité compétente destinataire garantit un niveau de protection adéquat**.

34. Le CEPD souligne que la CJUE a estimé, dans son avis 1/15 de juillet 2017 relatif à de tels transferts ultérieurs, que l'exigence visant à assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union *«vaut, de même, dans le cas de la communication des données PNR depuis le Canada vers d'autres pays tiers (...) afin d'éviter que le niveau de protection prévu par cet accord puisse être contourné par des transferts de données à caractère personnel vers d'autres pays tiers et de garantir la continuité du niveau de protection offert par le droit de l'Union»*[50]. La Cour a ajouté qu'*«une telle communication nécessite l'existence soit d'un accord entre l'Union et le pays tiers concerné équivalent audit accord, soit d'une décision de la Commission, au titre de l'article 25, paragraphe 6, de la directive 95/46, constatant que ledit pays tiers assure un niveau de protection adéquat au sens du droit de l'Union et couvrant les autorités vers lesquelles le transfert des données PNR est envisagé»*. Par conséquent, **le CEPD recommande d'ajouter cette exigence supplémentaire au paragraphe 16, point d), des directives de négociation**.

4.3. Droits des personnes concernées

35. Le CEPD prend note du fait que l'annexe n'inclut aucune directive spécifique concernant les droits des personnes concernées. Avant toute chose, le CEPD tient à rappeler que les droits d'accès et de rectification sont inscrits à l'article 8, paragraphe 2, de la charte en tant qu'éléments essentiels du droit à la protection des données. Si l'exercice des droits des personnes concernées est généralement limité dans le contexte répressif afin d'éviter de compromettre les enquêtes en cours, la possibilité pour les personnes concernées d'exercer leurs droits devrait exister dans la pratique et ne pas rester purement théorique, même si cet exercice est limité ou confié à un tiers de confiance dans des situations dans lesquelles l'exercice de ces droits est refusé pour protéger des informations sensibles en matière répressive.

36. L'accord-cadre comprend des dispositions relatives au droit à être informé (article 20), au droit d'accès (article 16), au droit de rectification - qui comprend également le droit d'effacement et le droit d'opposition (article 17) et le droit de ne pas faire l'objet de décisions automatisées (article 15). **Comme il a été soulevé dans l'avis relatif à l'accord-cadre[51], le CEPD considère que les exemptions prévues dans l'accord-cadre concernant l'exercice du droit à être informé et du droit d'accès sont si considérables qu'elles pourraient entraver l'exercice desdits droits.**

37. En ce qui concerne le droit d'accès, le CEPD estime que l'accord envisagé devrait s'assurer que la possibilité pour les personnes concernées d'accéder à leurs propres données existe effectivement, même si elle est limitée ou confiée à un tiers de confiance.

38. En ce qui concerne le droit à être informé, le CEPD remarque que le paragraphe 17, point e), des directives de négociation prévoit *«les garanties de confidentialité dont jouissent les autorités et les fournisseurs de services, y compris les exigences de non-divulgation»*. Le droit à l'information est de la plus haute importance, car il permet l'exercice d'autres droits

en matière de protection des données, y compris le droit à un recours, et garantit un traitement loyal des données[52]. Les personnes concernées n'ont généralement aucune connaissance du fait que leurs données sont traitées (ou transférées) à des fins répressives. Le CEPD rappelle que la CJUE, dans son avis 1/15, a jugé qu'*«il importe que les passagers aériens soient informés du transfert de leurs données PNR vers le Canada et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par les autorités publiques», considérant qu'«une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données PNR les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la charte, un recours effectif devant un tribunal»*[53].

39. Par conséquent, **le CEPD recommande d'inclure le droit à être informé et le droit d'accès dans les directives de négociation afin que les parties à l'accord redoublent d'efforts pour veiller à ce que les restrictions à l'exercice du droit d'accès soient limitées de façon sélective à celles qui sont indispensables pour défendre les intérêts généraux poursuivis et pour renforcer l'obligation de transparence qui incombe aux autorités compétentes**.

4.4. Contrôle d'une autorité indépendante

40. L'article 16 du TFUE et l'article 8, paragraphe 3, de la charte prévoient une garantie essentielle du droit à la protection des données, à savoir le contrôle exercé par une autorité indépendante. Bien que chaque État membre ait désigné une autorité indépendante chargée de contrôler les activités de traitement de données, y compris le transfert de données vers des pays tiers, il est en outre nécessaire de garantir une surveillance indépendante efficace une fois que les données ont été transférées dans les pays tiers destinataires.

41. L'article 21 de l'accord-cadre impose aux États-Unis d'Amérique de mettre en place une ou plusieurs autorités publiques de contrôle qui doivent *«exerce[r] en toute indépendance des fonctions et des pouvoirs de contrôle»*. Les États-Unis d'Amérique doivent prévoir un contrôle de manière cumulative par l'intermédiaire de plusieurs autorités, telles que notamment *«les inspecteurs généraux (inspectors general), les directeurs généraux chargés de la protection de la vie privée (chief privacy officers), l'organisme d'audit du Congrès (Government Accountability Office), la commission de surveillance du respect de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board) et d'autres organes exécutifs et législatifs de contrôle du respect de la vie privée ou des libertés civiles»*. Le CEPD rappelle que, conformément à la jurisprudence de la CJUE[54], une autorité de contrôle indépendante au sens de l'article 8, paragraphe 3, de la charte est une autorité capable de prendre des décisions indépendamment de toute influence extérieure, directe ou indirecte. Une telle autorité de contrôle doit non seulement être indépendante des parties qu'elle contrôle, mais elle ne doit pas non plus être *«subordonnée à une autorité de tutelle, dont elle peut recevoir des instructions»*, car cela signifierait qu'elle *«n'est donc pas à l'abri de toute influence extérieure susceptible d'orienter ses décisions»*[55].

42. **Le CEPD recommande de déterminer clairement, dans l'accord lui-même, la ou les autorités spécifiques chargées par les États-Unis d'Amérique de contrôler de manière indépendante le respect des règles posées par le traité envisagé**. L'accord devrait également préciser les pouvoirs effectifs que cette ou ces autorités spécifiques peuvent

exercer sur les autorités auxquelles les données à caractère personnel sont transférées sur la base de l'accord.

4.5. Recours juridictionnel et administratif

43. Le CEPD salue le fait que le mandat de négociation prévoit que *«[l]'accord devrait comporter une clause permettant aux personnes concernées de former des recours juridictionnels effectifs pendant la procédure pénale»*[56].

44. Le CEPD rappelle que la CJUE a conclu que [57] l'absence de possibilité d'exercer un recours juridictionnel lors du transfert de données à caractère personnel vers un pays tiers touche à l'essence même de l'article 47 de la charte, qui prévoit le droit à une protection juridictionnelle effective. Dans ce contexte, la CJUE a jugé qu'«*une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la charte*» et que «*l'article 47, premier alinéa, de la charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés ait droit à* ***un recours effectif*** *devant un tribunal dans le respect des conditions prévues à cet article*»[58].

45. En outre, la CJUE a souligné qu'il était essentiel que les personnes puissent introduire des plaintes auprès d'autorités de contrôle indépendantes[59] et demander à exercer, par conséquent, un recours administratif.

46. L'accord-cadre comprend deux dispositions - les articles 18 et 19 - relatives aux recours administratifs et juridictionnels. Comme il l'a soulevé dans son avis relatif à l'accord-cadre[60], le CEPD continue de nourrir de sérieuses inquiétudes quant à la conformité de l'article 19 avec la charte. Il est conscient que les États-Unis d'Amérique ont adopté en février 2016 une loi portant sur les recours juridictionnels, le *Judicial Redress Act*[61], qui étend certains droits au recours juridictionnel aux citoyens de pays désignés. Toutefois, il a besoin de davantage d'informations concernant la **nature effective** de tels recours juridiques, puisqu'il s'agit d'une exigence de l'article 47 de la charte, fondées sur un examen de la manière dont cet accord est mis en œuvre dans le droit américain et respecté dans les faits.

47. Par conséquent, **le CEPD recommande d'inscrire dans le mandat de négociation le fait que l'accord envisagé doit permettre que les deux voies de recours soient accessibles à toutes les personnes concernées**.

4.6. Catégories de personnes concernées

48. Les directives de négociation prévoient que *«[l]'accord devrait être réciproque pour ce qui est des catégories de personnes dont les données ne doivent pas être demandées en vertu de l'accord»*[62].

49. Le CEPD constate que le *CLOUD Act* fait référence à des personnes appelées «ressortissants américains» et opère des distinctions sur ce fondement. Par exemple, il ne permet pas aux fournisseurs de services étrangers de s'opposer aux injonctions émises par

les autorités répressives américaines sur la base d'un conflit de lois lorsque la personne dont les données sont demandées est un «ressortissant américain»[63].

50. Le CEPD rappelle la protection conférée par les articles 7 et 8 de la charte, aux termes lesquels les droits fondamentaux à la vie privée et à la protection des données à caractère personnel s'appliquent à «toute personne» au sein de l'Union européenne, indépendamment de sa nationalité ou de son statut. De la même manière, le RGPD n'établit pas de distinction fondée sur la nationalité ou le statut et garantit le même niveau de protection aux données à caractère personnel des citoyens et des résidents de l'Union qu'aux personnes non ressortissantes de l'Union ou n'y résidant pas. Par conséquent, le CEPD considère qu'il serait inacceptable d'opérer, dans l'accord envisagé, une quelconque distinction relativement au niveau de protection des données et aux garanties prévues pour le traitement de données à caractère personnel relevant du champ d'application du RGPD sur le fondement de la nationalité américaine ou de la résidence aux États-Unis d'Amérique de la personne concernée. **Le CEPD recommande de préciser, dans les directives de négociation, que toutes les personnes concernées par le traitement de leurs données au titre de l'accord devraient bénéficier du même niveau de protection des données et de garanties similaires.**

4.7. Définition et types de données

51. Les directives de négociation prévoient que *«[l]'accord devrait énoncer les définitions et les types de données à couvrir, incluant à la fois les données relatives au contenu et les données non relatives au contenu»*[64]. Le CEPD salue le fait que l'accord envisagé prévoie des définitions des catégories de données qui seraient couvertes. Il estime que la distinction entre données relatives au contenu et données non relatives au contenu ne saurait suffire à elle seule, puisque les deux types de données peuvent avoir un caractère également sensible.

52. À cet égard, le CEPD rappelle tout d'abord que la CJUE a conclu que l'accès aux données relatives au contenu est susceptible de porter atteinte à l'essence même du droit à la vie privée[65].

53. En ce qui concerne les données non relatives au contenu, la CJUE a conclu, à propos des métadonnées, telles que les données relatives au trafic et les données de localisation, conservées par des fournisseurs de communications électroniques accessibles au public, que *«prises dans leur ensemble, [de telles données] sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci»*[66] et *«fournissent les moyens d'établir [...] le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications»*[67].

54. **Le CEPD souligne l'importance de définir de manière claire et directe les catégories de données concernées par l'accord envisagé afin de garantir la sécurité juridique** à toutes les parties prenantes associées à l'Union et aux États-Unis d'Amérique - aspect qui fait partie du premier objectif énoncé dans le paragraphe 1 du mandat de négociation. L'efficacité des injonctions visant à obtenir des preuves électroniques pourrait être aisément compromise par un manque de précision et de clarté dans les définitions essentielles contenues dans l'accord envisagé. Dans la mesure où les définitions de catégories de

données énoncées dans la proposition relative aux preuves électroniques serviront de référence, comme l'a soulevé précédemment le comité européen de la protection des données[68], **le CEPD recommande de délimiter clairement les différentes catégories de données et d'éviter les chevauchements. Une telle approche contribuerait grandement à garantir la sécurité juridique** en ce qui concerne les dispositions matérielles de l'accord.

4.8. Infractions pénales couvertes par l'accord

55. Le CEPD salue le fait que les directives de négociation prévoient que *«[l]'accord devrait définir son champ d'application exact pour ce qui est des infractions pénales couvertes et des seuils»*[69]. En outre, le paragraphe 17, point b), précise que l'accord devrait prévoir *«les conditions adéquates pour garantir la nécessité et la proportionnalité des injonctions émises en vue d'obtenir un accès à des preuves électroniques, une distinction étant notamment établie entre les catégories de données, le cas échéant»*[70].

56. Le CEPD estime qu'il convient, pour se conformer à la condition de proportionnalité prévue à l'article 52, paragraphe 1, de la charte, de trouver un juste équilibre entre les types d'infractions pour lesquels la production et le transfert de données à caractère personnel pourraient être ordonnées, d'une part, et les catégories de données concernées, d'autre part. Ainsi, les distinctions devraient être également fondées sur la gravité des infractions sur lesquelles portent les enquêtes ou les poursuites, ainsi que sur le caractère sensible des catégories de données recherchées. **Le CEPD recommande donc de préciser, au paragraphe 17, point b, des directives de négociation, que les distinctions devraient également se fonder sur la gravité des infractions concernées**.

57. Le CEPD rappelle que, selon la jurisprudence de la CJUE, seul l'objectif de lutte contre les crimes graves peut justifier l'accès des autorités publiques aux données à caractère personnel conservées par les fournisseurs de service, données qui, *«prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées»*[71]. Lorsqu'il n'est pas possible de tirer de telles conclusions, et qu'on ne peut par conséquent considérer l'ingérence comme sérieuse, la Cour a en outre conclu que*«un accès à de telles données est donc susceptible d'être justifié [...] par l'objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales en général", [...] sans qu'il soit nécessaire que ces infractions soient qualifiées de "graves"»*[72]. Dès lors, il convient, au titre de l'accord envisagé, de limiter aux seuls crimes graves la possibilité d'ordonner la production et le transfert de données relatives ou non relatives au contenu, qui, prises dans leur ensemble, peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes concernées.

4.9. Sécurité de l'information

58. Conformément à l'article 9 de l'accord-cadre, l'Union européenne et les États-Unis d'Amérique sont tenus de *«mettre en place des dispositifs techniques, organisationnels et de sécurité afin de protéger les informations à caractère personnel»*. Les directives de négociation prévoient *«des garanties supplémentaires tenant compte [...] des exigences spécifiques d'un transfert de preuves électroniques effectué directement par des fournisseurs de services plutôt qu'entre autorités»*[73]. Parmi ces garanties spécifiques, le paragraphe 16, point f), prévoit que *«la notification d'un incident relatif à la sécurité des informations à l'autorité compétente désignée par l'État membre dans lequel le fournisseur de services est établi ou représenté s'effectuera dans les conditions énoncées à l'article 10, paragraphe 2, de l'accord-cadre»*.

59. Compte tenu du modèle de coopération directe entre les fournisseurs de services et les autorités judiciaires des deux côtés de l'Atlantique, le CEPD estime que l'accord envisagé soulève d'importantes questions concernant la sécurité des transmissions transfrontières, tant entrantes que sortantes, de données à caractère personnel en relation avec l'exécution d'injonctions relatives à l'obtention de preuves électroniques. Le CEPD souhaite souligner que garantir la sécurité des données à caractère personnel est non seulement une exigence claire du droit de l'Union[74], mais est aussi reconnu par la CJUE comme un caractère essentiel du droit fondamental à la protection des données à caractère personnel. En outre, la sécurité des données est primordiale afin de garantir le secret des enquêtes et la confidentialité des procédures pénales.

60. Par conséquent, **le CEPD recommande que le mandat de négociation inclue des garanties supplémentaires en vue d'assurer un niveau de sécurité approprié aux données à caractère personnel produites et transférées. Outre le paragraphe 16, point f), le mandat de négociation devrait aborder, en particulier, la question de la nécessité de garantir l'authenticité des injonctions et la sécurité des transmissions de données à caractère personnel aux autorités requérantes**.

4.10. Autorités compétentes pour émettre des injonctions

61. Le CEPD considère que l'accord envisagé devrait déterminer clairement les autorités des deux parties qui seraient compétentes pour émettre des injonctions adressées directement aux fournisseurs de services. Le CEPD remarque que cette question n'est pas spécifiquement abordée dans les directives de négociation. Dès lors, **il recommande d'inclure dans le mandat de négociation la nécessité de déterminer, dans l'accord, les autorités susceptibles d'émettre des injonctions relatives à l'obtention de preuves électroniques**.

62. Le CEPD souligne que le respect du principe de limitation de la finalité est étroitement lié au champ de compétences des destinataires dans le pays tiers destinataire. Pour garantir le respect du principe de limitation de la finalité, le champ de compétences des autorités des États-Unis d'Amérique auxquelles les données seront transmises et qui traiteront ces données devrait être clairement défini afin de s'assurer qu'elles sont également compétentes au regard des finalités du transfert. Dès lors, en ce sens, le CEPD **recommande que l'accord envisagé soit suivi d'une liste exhaustive des autorités américaines compétentes auxquelles les données pourront être transmises, accompagnée d'une brève description de leurs compétences. Cette préoccupation devrait également apparaître dans l'une des directives de l'annexe.**

4.11. Possibilité pour les fournisseurs de services de s'opposer à une injonction

63. Les fournisseurs de services qui reçoivent une injonction relative à l'obtention de preuves électroniques adressée par les autorités judiciaires américaines pourraient se trouver pris entre des obligations légales contradictoires, l'une relevant du droit de l'Union et l'autre du droit américain. Le CEPD salue le fait que le paragraphe 9 des directives de négociation prévoit que *«[l]'accord devrait également définir les circonstances dans lesquelles un fournisseur de services a le droit de s'opposer à une injonction»*.

64. À cet égard, le CEPD remarque que le *CLOUD Act* américain permet aux fournisseurs de services étrangers, et uniquement dans certains cas limités, de s'opposer aux injonctions émanant des autorités répressives américaines sur la base d'un conflit de lois. Il leur est permis de déposer devant les tribunaux américains une demande appelée «requête en annulation» («motion to quash»), à la double condition que l'abonné ou le client dont les données sont requises ne soit pas un ressortissant américain et ne réside pas aux États-Unis d'Amérique, d'une part, et que l'injonction soulève un conflit de lois avec un gouvernement étranger répondant à certains critères[75].

65. **Le CEPD considère que les fournisseurs de services à qui une injonction relative à l'obtention de preuves électroniques a été délivrée devraient avoir la possibilité de s'opposer à cette injonction, sur le fondement de motifs spécifiques définis dans l'accord envisagé, tels que des informations manquantes ou inexactes, ou des considérations relatives aux droits fondamentaux[76].** De tels motifs devraient être clairement définis de manière à ce que les fournisseurs de services ne puissent décider, au cas par cas, d'accepter ou de refuser de coopérer, ou des modalités de cette coopération. Par conséquent, plutôt que de définir «en quelles circonstances», **le CEPD recommande de préciser, dans les directives de négociation, que l'accord doit également définir «les motifs spécifiques que les fournisseurs de services peuvent invoquer pour s'opposer à une injonction».**

5. CONCLUSIONS

66. Le CEPD comprend que les autorités répressives doivent pouvoir recueillir et obtenir des preuves électroniques rapidement et efficacement. Le CEPD soutient ces efforts visant à trouver des approches innovantes aux fins d'obtenir l'accès transfrontière aux preuves électroniques. Par conséquent, le présent avis vise à fournir des recommandations constructives et objectives aux institutions européennes alors que la Commission cherche à obtenir l'autorisation de Conseil de négocier avec les États-Unis d'Amérique.

67. Le CEPD partage l'opinion de la Commission selon laquelle l'accord envisagé devrait être subordonné à la mise en place de mécanismes forts de protection des droits fondamentaux. Les directives de négociation envisagent déjà un certain nombre de principes et de garanties relatifs à la protection des données. Il recommande tout d'abord d'inclure l'article 16 du TFUE dans les bases juridiques matérielles figurant en préambule de la décision du Conseil. Il salue le fait que l'accord-cadre, qu'il a activement soutenu, s'applique, par référence, au futur accord. Dans son avis 1/2016 relatif à l'accord-cadre, le CEPD préconise des améliorations essentielles ainsi que le renforcement de plusieurs garanties; il préconise que ces garanties soient incluses dans les directives de négociation.

68. Compte tenu de l'incidence de l'accord envisagé sur les droits fondamentaux, le CEPD considère en outre qu'au-delà des garanties envisagées dans les directives de négociation, certaines garanties supplémentaires devraient être incluses afin de s'assurer que l'accord final respecte l'exigence de proportionnalité. Il recommande en particulier que les autorités judiciaires désignées par l'autre partie à l'accord participent aussi tôt que possible au processus de collecte des preuves électroniques, afin que lesdites autorités puissent contrôler la conformité des injonctions aux droits fondamentaux et soulever des motifs de refus.

69. Outre ces recommandations générales, les recommandations et observations formulées par le CEPD dans le présent avis portent sur les aspects spécifiques suivants des futurs accords

internationaux à négocier avec les États-Unis d'Amérique dans le cadre des directives de négociation:

- le caractère obligatoire de l'accord;
- les transferts ultérieurs par les autorités américaines compétentes;
- les droits des personnes concernées aux États-Unis d'Amérique, notamment le droit à être informé et le droit d'accès;
- le contrôle par une autorité indépendante aux États-Unis;
- les recours juridictionnel et administratif aux États-Unis;
- les catégories de personnes concernées;
- la définition et le type de données couvertes par l'accord envisagé;
- les infractions pénales couvertes par l'accord envisagé;
- les garanties spécifiques destinées à assurer un niveau approprié de sécurité des données transférées;
- les types d'autorité pouvant émettre des injonctions relatives à l'obtention de preuves électroniques;
- la possibilité, pour les fournisseurs de services auxquels une injonction relative à l'obtention de preuves électroniques a été adressée, de s'opposer sur le fondement de motifs spécifiques.

70. Enfin le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus. Les commentaires du présent avis sont sans préjudice des observations supplémentaires que le CEPD pourrait faire ultérieurement, notamment si de nouveaux problèmes étaient soulevés et abordés par le CEPD à la lumière d'informations complémentaires. Il s'attend à être consulté au sujet du texte du projet d'accord avant que celui-ci ne soit finalisé.

Bruxelles, le 2 avril 2019

Giovanni Buttarelli

Contrôleur européen de la protection des données

NOTES

[1] JO L 119 du 4.5.2016, p. 1 (ci-après le «RGPD»).
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119, 4.5.2016, p. 89 (ci-après la «directive relative à la protection des données dans le domaine répressif»).
[44] Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final.
[5] Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM(2018) 226 final.
[6]Le Conseil a adopté son orientation générale sur la proposition de règlement le 7 décembre 2018, disponible à l'adresse https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/. Le Conseil a adopté son orientation générale sur la proposition de directive le 8 mars 2018, disponible à l'adresse https://www.consilium.europa.eu/fr/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/
[7] Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.
[8] Recommandation de décision du Conseil autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (SCTE nº 185), COM(2019) 71 final; convention sur la coopération internationale renforcée sur la cybercriminalité et les preuves électroniques, Budapest, 23 novembre 2001, SCTE nº 185.
[9] Avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un second protocole additionnel à la convention de Budapest sur la cybercriminalité.
[10] Accord du 25 juin 2003 entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, JO L 181, 19.7.2003, p. 34.
[11] Dans de récentes décisions et affaires judiciaires aux États-Unis d'Amérique, les tribunaux ont tenté de préciser si les autorités américaines avaient le droit de demander la production de données stockées à l'étranger par un fournisseur de services relevant de la juridiction des États-Unis. Parmi ces affaires, la fameuse affaire Microsoft Ireland a été portée jusque devant la Cour suprême des États-Unis après que Microsoft ait refusé d'exécuter une ordonnance américaine l'enjoignant de divulguer des données stockées sur ses serveurs en Irlande et ait contesté l'application du *Stored Communications Act*. Le 23 mars 2018, les États-Unis d'Amérique ont adopté le *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. D'une part, le *CLOUD Act* modifie le *Stored Communication Act* et précise que les pouvoirs des autorités répressives américaines d'ordonner la production de données s'applique «que de telles communications, enregistrements, ou autres informations soient situées aux États-Unis d'Amérique ou non». La loi a ainsi confirmé que le pouvoir des autorités répressives américaines de rendre des ordonnances aux fins de divulguer des données revêt une portée extraterritoriale, et a rendu l'affaire Microsoft Ireland sans objet. Elle inscrit également dans la législation américaine une pratique des autorités répressives américaines consistant à contourner les traités d'entraide judiciaire pénale actuellement en place entre les États-Unis d'Amérique et les pays étrangers, y compris le traité d'entraide judiciaire en vigueur entre l'Union et les États-Unis d'Amérique. D'autre part, le *CLOUD Act* donne la possibilité aux États-Unis d'Amérique de conclure des «accords exécutifs» avec des «gouvernements étrangers répondant à certains critères», ce qui permettrait aux autorités répressives de ces pays tiers de demander directement l'accès aux données aux États-Unis d'Amérique, sous certaines conditions.
[12] Voir titre 18, paragraphe 2702, du Code des États-Unis d'Amérique (ci-après «USC»).
[13] Document de travail des services de la Commission: Analyse d'impact, SWD(2018) 118 final, disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN.
[14] Disponible à l'adresse suivante: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.
[15] Voir titre 18, paragraphes 2511, 2523 et 2702, USC.
[16] Exposé des motifs de la recommandation, p. 4-5.
[17] Exposé des motifs de la recommandation, p. 4.
[18] Paragraphe 2 des directives de négociation.
[19] Arrêt du 30 avril 1974, Haegemann/État belge, affaire 181/73, ECLI:EU:C:1974:41, point 5.
[20] Arrêt de la CJUE du 3 septembre 2008, Kadi et Al Barakaat International Foundation/Conseil et Commission, affaires jointes C-402/05 P et C-415/05 P, ECLI:EU:C:2008:461, point 285. [soulignement ajouté].
[21]Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592.

[22] Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 214; voir également point 93.
[23] 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.
[24] Il s'agit d'une dérogation à l'article 35, paragraphe 1, point b), de la directive en matière de protection des données dans le domaine répressif, qui dispose que les données à caractère personnel sont transférées par les autorités répressives des États membres de l'Union à un responsable du traitement dans un pays tiers ou à une organisation internationale qui est également une autorité répressive.
[25] Les conditions supplémentaires sont les suivantes:
«1 (...) (a) le transfert est strictement nécessaire à l'exécution de la mission de l'autorité compétente qui transfère les données ainsi que le prévoit le droit de l'Union ou le droit d'un État membre aux fins énoncées à l'article 1er, paragraphe 1;
(b) l'autorité compétente qui transfère les données établit qu'il n'existe pas de libertés ni de droits fondamentaux de la personne concernée qui prévalent sur l'intérêt public nécessitant le transfert dans le cas en question;
(c) l'autorité compétente qui transfère les données estime que le transfert à une autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers est inefficace ou inapproprié, notamment parce que le transfert ne peut pas être effectué en temps opportun;
(d) l'autorité qui est compétente aux fins visées à l'article 1er, paragraphe 1, dans le pays tiers est informée dans les meilleurs délais, à moins que cela ne soit inefficace ou inapproprié;
(e) l'autorité compétente qui transfère les données informe le destinataire de la finalité ou des finalités déterminées pour lesquelles les données à caractère personnel ne doivent faire l'objet d'un traitement que par cette dernière, à condition qu'un tel traitement soit nécessaire. [...]
3. L'autorité compétente qui transfère les données informe l'autorité de contrôle des transferts relevant du présent article.
4. Lorsqu'un transfert est effectué sur la base du paragraphe 1, ce transfert est documenté».
[26] Voir également avis 23/2018 du 26 septembre 2018 du comité européen de la protection des données concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (ci-après l'«avis 23/2018 du comité européen de la protection des données»), p. 9, disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2018-09-26-eevidence_fr.pdf.
[27] Exposé des motifs de la recommandation, p. 7.
[28] Arrêt de la CJUE du 25 octobre 2017, Commission/Conseil (CMR-15), C-687/15, ECLI:EU:C:2017:803, point 48 et suivants.
[29] Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 232.
[30] Paragraphe 14 des directives de négociation.
[31] Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, JO L 336, 10.12.2016, p. 3 (ci-après l'«accord-cadre»).
[32] Ce cadre s'applique principalement aux transferts de données à caractère personnel entre l'Union et les autorités répressives américaines. Il peut également s'appliquer aux données à caractère personnel «transférées autrement conformément à un accord conclu entre les États-Unis et l'Union européenne ou ses États membres» à des fins répressives (article 3, paragraphe 1). Par conséquent, l'accord-cadre peut aussi couvrir les transferts de données de sociétés privées concernées lorsqu'ils sont basés sur des accords internationaux entre l'Union et les États-Unis d'Amérique, tels que des transferts effectués par des fournisseurs de services au titre de l'accord sur l'accès transfrontière aux preuves électroniques envisagé.
[33] Avis 1/2016 du CEPD du 12 février 2016 relatif à l'accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière (ci-après l'«avis 1/2016 du CEPD»), disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_fr.pdf.
[34] Voir sections 4.3, 4.4 et 4.5 ci-dessous.
[35]Le CEPD travaille actuellement sur des lignes directrices portant sur l'évaluation du caractère proportionnel des mesures qui limitent les droits fondamentaux à la vie privée et à la protection des données à caractère personnel. Une version provisoire de ces lignes directrices a été récemment soumise à la consultation des parties prenantes avant la publication de la version finale. Elles sont disponibles à l'adresse: https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[36] Exposé des motifs de la recommandation, p. 5.

[37] Voir sections 3.4, 4.2, 4.9 et 4.11 ci-dessous.
[38] Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, en particulier le point 134, dans lequel la Cour estime que *«[m]ême si les moyens visant à garantir un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union [...], ces moyens doivent néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union»*.
[39] Paragraphe 1 des directives de négociation.
[40] Voir liste de motifs d'objection mentionnés à l'article 14 de la proposition relative aux preuves électroniques, ainsi que jurisprudence développée par la CJUE dans le cadre du mandat d'arrêt européen (arrêt de la CJUE du 5 avril 2016, Aranyosi et Căldăraru, C-404/15 et C-659/15 PPU, ECLI:EU:C:2016:198, point 82 et suivants).
[41] Voir article 6 du traité sur l'Union européenne et l'article 67, paragraphe 1, du TFUE. Voir également avis du 14 février 2011 de l'Agence des droits fondamentaux relatif au projet de directive concernant la décision d'enquête européenne, note 56: «*dans ce contexte, il convient de rappeler le principe de responsabilité extraterritoriale au titre de la Convention européenne des droits de l'homme. Les États membres de l'Union sont responsables, au titre de la Convention européenne des droits de l'homme, des violations des droits de l'homme commises dans un autre territoire lorsque, à raison de leurs actes, ils ont exposé une personne à une telle situation; voir arrêt de la Cour européenne des droits de l'homme (ci-après la «CEDH») du 7 juillet 1989, Soering c. Royaume-Uni, nº 14038/88. Voir également CEDH, Bosphorus v. Ireland, nº 45036/98, 30 juin 2005, paragraphe 156: «il y a lieu de présumer qu'un État respecte les exigences de la [c]onvention lorsqu'il ne fait qu'exécuter des obligations juridiques résultant de son adhésion à l'[Union européenne].» La Cour a considéré qu'une telle présomption pouvait être renversée»*.
[42] Voir avis du 14 février 2011 de l'Agence des droits fondamentaux relatif au projet de directive concernant la décision d'enquête européenne, 14 février 2011, note 61 faisant référence à l'arrêt de la CEDH du 21 janvier 2011, M.S.S. c. Belgique et Grèce, nº 30696/09.
[43] Disponible à l'adresse suivante: http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/fr/pdf.
[44] Voir note 34 de l'orientation générale du Conseil «*La République tchèque, la Finlande, l'Allemagne, la Grèce, la Hongrie et la Lettonie ont émis une réserve sur la procédure de notification, préconisant qu'elle ait davantage d'effets et couvre aussi les données relatives aux transactions et la clause relative aux droits fondamentaux, autrement dit, qu'elle donne à l'autorité notifiée des motifs de refus. Par ailleurs, une logique inverse devrait être retenue pour déterminer ce qu'est un "cas national". Enfin, l'Allemagne préconise que l'injonction soit soumise et non le certificat, tandis que la République tchèque estime qu'il faudrait soumettre les deux».*
[45] Voir avis 23/2018 du comité européen de la protection des données, p. 16.
[46] Voir avis 23/2018 du comité européen de la protection des données, p. 17.
[47] Voir exposé des motifs de la recommandation, p. 8.
[48] Voir doc. prél. nº 10 de décembre 2008 -Le caractère obligatoire ou non obligatoire de la convention sur l'obtention des preuves [en matière civile ou commerciale]: https://assets.hcch.net/upload/wop/2008pd10e.pdf; et jugement de la Cour suprême des États-Unis d'Amérique dans l'affaire Société Nationale Industrielle Aérospatiale c. United States District Court for the Southern District of Iowa, 482 US 522, 535, 548 (1987).
[49] L'article 35, paragraphe 1, point b), dispose que le transfert ultérieur est effectué entre les autorités responsables de la prévention et de la détection des infractions pénales, et des enquêtes et des poursuites en la matière. L'article 35, paragraphe 1, point e), prévoit le principe d'autorisation préalable de l'État membre d'origine.
[50] Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 214.
[51] Avis 1/2016 du CEPD, points 39 et 41.
[52] Arrêt de la CJUE du 1er octobre 2015, Bara e.a., C-201/14, ECLI:EU:C:2015:638, en particulier les points 32 et 33, dans lesquels la Cour a conclu que *«cette exigence d'information des personnes concernées par le traitement de leurs données personnelles est d'autant plus importante qu'elle est une condition nécessaire à l'exercice par ces personnes de leur droit d'accès et de rectification des données traitées [...] et de leur droit d'opposition au traitement desdites données»* et que *«[c]es informations concernent l'identité du responsable du traitement de ces données, les finalités de ce traitement ainsi que toute information supplémentaire nécessaire pour assurer un traitement loyal des données»*.
[53]Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220. [soulignement ajouté].
[54] Voir arrêt de la CJUE du 9 mars 2010, Commission/Allemagne, C-518/07, ECLI:EU:C:2010:125, point 25; arrêt de la CJUE du 16 octobre 2012, Commission/Autriche, C-614/10, ECLI:EU:C:2012:631, points 36 et 37; arrêt de la CJUE du 8 avril 2014, Commission/Hongrie, C-288/12, point 48; arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 41.
[55] Avis 1/15 de la CJUE du 26 juillet 2017, Accord PNR UE-Canada, ECLI:EU:C:2017:592, point 230.
[56] Voir paragraphe 9 des directives de négociation.
[57] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 95.
[58] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 95. [soulignement ajouté].

[59] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, paragraphe 56-58.
[60] Avis 1/2016 du CEPD, point 46.
[61] Disponible à l'adresse suivante: https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.
[62] Paragraphe 13 des directives de négociation.
[63] Voir titre 18, paragraphe 2703, USC.
[64] Voir paragraphe 6 des directives de négociation.
[65] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 39.
[66] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 27.
[67] Arrêt de la CJUE du 21 décembre 2016, Tele2 Sverige, affaires jointes C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 99.
[68] Voir avis 23/2018 du comité européen de la protection des données, p. 12: *«En effet, les quatre catégories proposées ne semblent pas clairement délimitées et la définition des "données relatives à l'accès" reste encore vague par rapport aux autres catégories»*.
[69] Voir paragraphe 7 des directives de négociation.
[70] Voir paragraphe 17, point b), des directives de négociation.
[71] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, point 54, voir également le point 56.
[72] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, point 62. [soulignement ajouté].
[73] Voir paragraphe 15 des directives de négociation.
[74] Les données à caractère personnel devraient être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé ou illicite à ces données et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées[principe d'intégrité et de confidentialité consacré à l'article 5, paragraphe 1, point f), du RGPD, et à l'article 4, paragraphe 1, point f), de la directive relative à la protection des données dans le domaine répressif]. La sécurité du traitement comprend notamment la capacité à garantir de manière constante la confidentialité et l'intégrité des systèmes de traitement.
[75] Voir titre 18, paragraphe 2703, USC.
[76]Voir avis 23/2018 du comité européen de la protection des données, p. 17, dans lequel le comité recommande que «*doit au moins prévoir la dérogation classique minimale selon laquelle, s'il existe des motifs substantiels de croire que la mise en œuvre d'une injonction conduirait à une violation du droit fondamental de la personne concernée et que l'État chargé de la mise en œuvre ne s'acquitterait pas de ses obligations concernant la protection des droits fondamentaux reconnus dans la charte, la mise en œuvre de l'injonction doit être refusée»*.