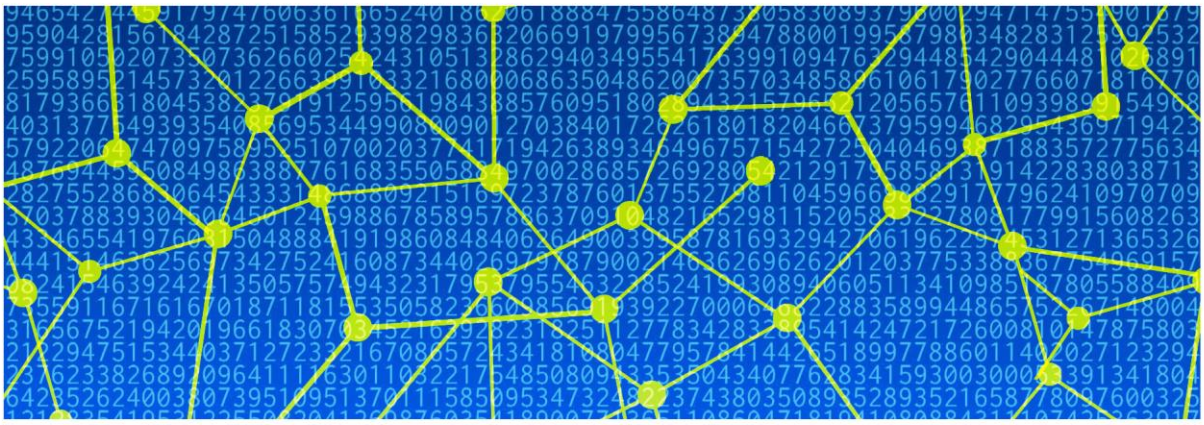

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 3/2019

Avis du CEPD relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité

EDPS

2 avril 2019

Le Contrôleur européen de la protection des données («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 en vertu 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 (TFUE) et respectent les droits fondamentaux qui forment le noyau du droit de l'Union. En particulier, il convient de veiller au respect des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 16 du TFUE.

Synthèse

Le 5 février 2019, la Commission européenne a publié une recommandation de décision du Conseil autorisant la Commission à participer au nom de l'Union européenne aux négociations d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité. L'annexe de la recommandation définit les directives recommandées du Conseil pour la négociation du protocole. Ledit protocole vise à améliorer les moyens traditionnels de coopération et à inclure des dispositions pour une coopération directe entre les autorités répressives et les prestataires de services transfrontaliers, ainsi que des dispositions sur l'accès transfrontalier direct aux données par les autorités répressives.

Le CEPD salue et soutient activement la recommandation visant à autoriser la Commission européenne à négocier, au nom de l'Union européenne, un deuxième protocole additionnel à la convention sur la cybercriminalité. 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 les traités de l'Union et 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», parce que les informations sont stockées au format électronique dans un pays tiers. Le volume croissant de demandes 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 aux institutions de l'Union alors que le Conseil doit émettre ses directives avant que cette tâche délicate ne commence et n'entraîne d'importantes conséquences. Le CEPD souligne le besoin de garantir le plein respect des droits fondamentaux, en ce compris à la vie privée et à la protection des données à caractère personnel. Même si le CEPD reconnaît qu'il est impossible de transposer entièrement la terminologie et les définitions du droit de l'Union dans un accord avec des pays tiers, il insiste sur le fait que les garanties des particuliers doivent être claires et efficaces afin de pleinement respecter le droit primaire de l'Union. Ces dernières années, la Cour de justice de l'Union européenne a confirmé 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.

De nombreuses garanties déjà envisagées sont saluées, mais devraient être renforcées. Le CEPD a défini trois améliorations principales qu'il recommande pour les directives de négociation, afin de garantir le respect de la charte et de l'article 16 du TFUE:

- garantir le caractère obligatoire du protocole envisagé,
- introduire des garanties détaillées – en ce compris le principe de limitation des finalités – étant donné la multitude de signataires potentiels, tous ne constituant pas parties à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ou n'ayant pas conclu d'accord équivalent à l'accord-cadre UE-US,
- s'opposer à toutes dispositions sur l'accès direct aux données.

En outre, l'avis émet des recommandations supplémentaires relatives à des améliorations et des éclaircissements 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 protocole.

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 et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale[7], ainsi qu'une recommandation d'autoriser la Commission, au nom de l'Union européenne, à participer aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STCE nº 185) (ci-après la «recommandation»)[8]. La première 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 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 pour le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité (SCTE nº 185)[10], selon les directives de négociation annexées à la recommandation. 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 le protocole au nom de l'Union européenne. 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 à la suite de l'adoption de la recommandation par la Commission européenne en vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725. Le CEPD salue également la référence faite à son avis dans le considérant 8 de la recommandation. Il souhaite souligner que cet avis est sans préjudice de tout commentaire supplémentaire que le CEPD pourrait émettre sur la base d'autres informations disponibles, des dispositions du projet de protocole dans le cadre des négociations et des avancées législatives au sein de pays tiers.

2. OBJECTIFS DU DEUXIÈME PROTOCOLE ADDITIONNEL

5. La convention du Conseil de l'Europe sur la coopération internationale renforcée sur la cybercriminalité et les preuves électroniques (ci-après la «**convention sur la cybercriminalité**») est ouverte aux États membres du Conseil de l'Europe, ainsi qu'à ceux qui n'en sont pas membres (sur invitation). À l'heure actuelle, 62 pays sont parties à la convention, en ce compris 26 États membres de l'Union (tous sauf l'Irlande et la Suède, qui l'ont signée) et d'autres pays tiers membres du Conseil de l'Europe comme l'Arménie, l'Azerbaïdjan, la Turquie ainsi que des pays non-membres du Conseil de l'Europe, comme l'Australie, le Canada, le Ghana, Israël, le Japon, le Maroc, le Paraguay, les Philippines, le Sénégal, le Sri Lanka, le Royaume de Tonga et les États-Unis[11]. La convention sur la cybercriminalité n'est pas ouverte à la signature par l'Union européenne.

6. La convention sur la cybercriminalité est un instrument international contraignant requérant des parties contractantes qu'elles définissent des infractions pénales spécifiques commises à l'encontre de réseaux électroniques ou au moyen desdits réseaux dans leur législation nationale et définissent également des pouvoirs et procédures spécifiques autorisant leurs autorités nationales à mener leurs enquêtes pénales, en ce compris en collectant des preuves électroniques. Elle prévoit des exigences minimales relatives aux pouvoirs d'enquête disponibles dans une enquête pénale. La convention sur la cybercriminalité encourage également la coopération internationale entre les parties contractantes.

7. Dans sa note d'orientation nº 3 adoptée en 2014[12], le comité de la convention sur la cybercriminalité (ci-après le «T-CY») a déclaré que *«[d]ans l'ensemble, les pratiques, les procédures ainsi que les conditions et les garanties qui les accompagnent varient considérablement entre les différentes parties. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données à caractère personnel, la base légale de l'accès aux données*

stockées à l'étranger ou au moyen de l'informatique en nuage, et le principe de la souveraineté nationale».

8. En juin 2017, afin de trouver une solution aux défaillances et aux ambigüités du cadre de la convention, les parties à la convention sur la cybercriminalité ont décidé de commencer à travailler sur un **deuxième protocole additionnel** à la convention, afin de finaliser le processus d'ici fin 2019[13]. Le protocole peut inclure:
    - **Dispositions en faveur d'une entraide judiciaire pénale plus efficace**:
        - un régime simplifié pour les demandes d'entraide judiciaire pénale relativement aux informations d'abonnés;
        - des injonctions internationales de production;
        - une coopération directe entre les autorités judiciaires dans le cadre des demandes d'entraide judiciaire pénale;
        - des enquêtes conjointes et des équipes communes d'enquête;
        - des demandes en anglais;
        - des auditions de témoins, de victimes et d'experts audio/vidéo;
        - des procédures d'entraide judiciaire d'urgence.
    - **Dispositions permettant une coopération directe avec les prestataires de services**[14] dans d'autres juridictions concernant des demandes d'**informations d'abonnés, de conservation des demandes et des demandes d'urgence.**
    - Un cadre plus transparent et des garanties plus importantes pour les pratiques existantes **d'accès transfrontalier aux données**[15].
    - **Garanties, y compris les exigences en matière de protection des données**[16].

    La Commission européenne participe à des séances plénières du T-CY en tant qu'observateur.

3. RECOMMANDATIONS PRINCIPALES

3.1. Mandat au niveau de l'Union et caractère obligatoire du protocole

9. Selon la Commission, le protocole «*est directement lié aux règles communes de l'UE en vigueur et à leurs perspectives d'évolution*». Lorsque les négociations seront conclues, le protocole «*pourrait in fine contenir des mesures portant sur des domaines dans lesquels l'Union a déjà adopté des dispositions législatives, comme la coopération judiciaire et la protection des droits fondamentaux*». Les négociations sur le protocole «*peuvent également être en lien avec la législation future de l'Union – en particulier concernant l'accès transfrontière aux preuves électroniques*»[17] (la proposition relative aux preuves électroniques susmentionnée). Il est important que l'Union participe aux négociations visant à définir ce protocole. Compte tenu de l'importance des sujets discutés à l'échelle internationale pour la politique de l'Union en matière de collecte de preuves électroniques dans le domaine pénal, en particulier concernant la protection des données à caractère personnel et la vie privée, et le stade d'ores et déjà avancé du débat après deux ans de négociations, **le CEPD soutient vivement l'adoption d'une décision du Conseil conférant un mandat clair à la Commission européenne** afin qu'elle puisse participer, au nom de l'Union, aux négociations en cours. La Commission serait la mieux placée pour veiller à la compatibilité du protocole avec la législation actuelle et future de l'Union. Ce mandat devrait permettre à l'Union européenne ainsi qu'à ses États membres de mieux garantir la légalité de l'accord à venir au sein de l'ordre juridique de l'Union, en ce compris

le respect de la charte des droits fondamentaux de l'Union (ci-après la «charte»), en particulier les droits à la vie privée et à la protection des données à caractère personnel, et de l'article 16 du TFUE. Par conséquent, le présent avis vise à fournir des conseils constructifs et objectifs aux institutions de l'Union. Le CEPD restera à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus.

10. Étant donné que les divers accords internationaux prévoyant des échanges de preuves transfrontières ont des incidences sur les droits fondamentaux à la protection de leurs données à caractère personnel et à la vie privée des personnes concernées, il est important que le cadre légal dans lequel ils opèrent soit défini de façon aussi transparente que possible. Il résulte du **point e)** de l'annexe que le protocole «*peut s'appliquer en l'absence d'autres accords internationaux plus spécifiques qui lient l'Union européenne ou ses États membres et d'autres parties à la convention, ou, si de tels accords internationaux existent, uniquement dans la mesure où certaines questions ne sont pas régies par ceux-ci*»[18]. L'utilisation du verbe «pouvoir» («peut») crée une ambiguïté quant à la nature du protocole envisagé. **Afin d'assurer la sécurité juridique, le CEPD recommande de clarifier le caractère contraignant et obligatoire de l'instrument en tant que principe**[19] et en fonction des accords bilatéraux entre les parties au protocole conclu à ce propos «*dès lors qu'ils sont compatibles avec les objectifs et les principes de la convention*». **Il convient de préciser que de tels accords bilatéraux concernent également de futurs accords, tels que précisés dans l'exposé des motifs de la recommandation[20]. Pour le CEPD, ceci est uniquement nécessaire lorsque l'autre accord international spécifique prévoit un degré de protection de la vie privée et des données à caractère personnel semblable ou supérieur au protocole envisagé**.

3.2. Le besoin de garanties détaillées concernant les transferts internationaux de données et le respect des droits fondamentaux

11. La Cour de justice de l'Union européenne (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 communautaires doivent respecter les droits fondamentaux, ce respect constituant une condition de leur légalité*»[21].

12. Le CEPD considère que des garanties appropriées concernant le droit à la protection des données requièrent avant tout **une compatibilité parfaite avec l'article 8 de la charte dans les pays tiers vers lesquels seraient transférées les données à caractère personnel.** Il souligne que, conformément à la jurisprudence de la CJUE, les articles 7 et 8 de la charte doivent être étudiés conjointement au **droit à un recours effectif prévu à l'article 47 de la charte**[22].

13. **Le CEPD se réjouit de l'attention accordée à la vie privée et à la protection des données dans l'annexe**. Le CEPD partage en effet la vision selon laquelle les garanties devraient s'appliquer à «*tous les pouvoirs d'investigation, que ceux-ci existent dans le cadre de la convention ou qu'ils soient instaurés par le deuxième protocole additionnel*»[23]. **Les points b) et c),** en particulier, semblent opposer la protection des données à caractère personnel à la protection des données de communication électronique. Le CEPD recommande de préciser que le protocole envisagé devrait veiller au respect des droits fondamentaux à la vie privée, d'une part, et à la protection des données à caractère

personnel, d'autre part, que ces dernières constituent ou non des données de communication électronique.

14. **La limite des finalités** est un principe essentiel de la protection des données. Les directives de négociation recommandées ne précisent aucune limite à la coopération dans le cadre du protocole envisagé et ne contiennent aucune limite spécifique concernant le traitement complémentaire des données à caractère personnel transférées par l'autorité requérante du pays tiers. **Le CEPD recommande de préciser plus rigoureusement les finalités des transferts dans l'annexe et l'interdiction de traitements supplémentaires incompatibles avec lesdites finalités.**

15. Le CEPD souligne que le respect de ce principe est étroitement lié au champ de compétences des bénéficiaires dans les pays tiers destinataires. Le champ de compétences des autorités spécifiques de pays tiers 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 le protocole envisagé s'accompagne d'une liste exhaustive des autorités compétentes des pays tiers destinataires auxquelles les données pourront être transmises ainsi que d'une brève description de leur compétences. Cette recommandation devrait également apparaître dans l'une des directives de l'annexe.**

16. En outre, envoyer ou répondre à des demandes de production de données dans le cadre du protocole envisagé entraînerait le **transfert de données à caractère personnel.** En juillet 2017, dans son avis 1/15[24] 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»*[25]. **Par conséquent, il résulte de l'avis 1/15 que le niveau de protection découlant des accords internationaux envisagés avec les pays tiers sur l'échange de données à caractère personnel avec des pays tiers 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.**

17. À cet égard, le CEPD souligne que tandis que tous les États membres sont parties à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après la «convention 108»)[26] du Conseil de l'Europe, applicable dans le domaine de la répression, tous les pays tiers parties à la convention sur la cybercriminalité ne sont pas parties à ladite convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[27]. Il est donc **particulièrement urgent de garantir l'ajout de garanties solides et détaillées dans le protocole envisagé**. En outre, le CEPD attire l'attention sur l'importance de collecter des informations sur le niveau de protection des données à caractère personnel des pays tiers participant à la convention sur la cybercriminalité[28] ainsi que sur leur contexte politique**, afin de pouvoir définir les garanties précises nécessaires.**

3.3. Accès direct des autorités répressives aux données

18. Selon la recommandation[29], «*il est possible que le deuxième protocole additionnel contienne des dispositions relatives à "l'extension des recherches et l'accès sur la base des pouvoirs"*[30] *et aux "techniques d'enquête"*». Dans son analyse d'impact sur la proposition relative aux preuves électroniques, la Commission a étudié la possibilité d'introduire une disposition relative à l'accès direct à l'échelle de l'Union et a décidé de ne pas donner suite. Il résulte toutefois de la recommandation[31] que la Commission estime que l'adoption d'un train de mesures concernant les preuves électroniques sur la base de ses propositions n'empêcherait pas les États membres de conserver ou d'adopter de telles mesures[32].

19. Le CEPD indique que les garanties sont envisagées dans le mandat en vertu du **point m) de l'annexe**. Toutefois, **le CEPD considère cette mesure comme particulièrement intrusive et, par conséquent, comme ayant davantage d'incidence sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel**. Ainsi, sans autres clarifications des mesures spécifiques et garanties plus strictes envisagées, **il recommande de s'opposer à l'introduction desdites dispositions dans le protocole**. Il se réfère à cet égard aux commentaires du groupe de travail «article 29» sur la question de l'accès direct des autorités répressives des pays tiers aux données stockées dans d'autres juridictions, comme le propose le projet d'éléments pour un protocole additionnel à la convention de Budapest sur la cybercriminalité[33]. Il est contre le **point n) de l'annexe** selon lequel l'Union européenne «*devrait également veiller à ne pas restreindre les possibilités d'un tel accès qui sont actuellement prévues dans les États membres*».

4. RECOMMANDATIONS COMPLÉMENTAIRES

20. Le CEPD souhaite exprimer les observations générales et les recommandations spécifiques suivantes sur les directives de négociation figurant dans l'annexe des recommandations. Le CEPD se réjouit que plusieurs directives concernent l'adoption de garanties de protection des données adéquates. Il considère que ces principes et garanties devraient être davantage précisés et renforcés.

21. 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 ce protocole avec les pays tiers devraient prévoir et atténuer ces risques de manière satisfaisante.

4.1. Base juridique de la décision du Conseil

22. L'exposé des motifs de la recommandation établit que «*[l]'objet du deuxième protocole additionnel relève [...] notamment dans le domaine des instruments relatifs à la coopération judiciaire en matière pénale (article 82, paragraphe 1, du TFUE) et à la protection des données (article 16 du TFUE)*»[34]. Ces deux dispositions sont également mentionnées au considérant 6 de la recommandation, selon lequel «*[l]'article 82, paragraphe 1, et l'article 16 du traité sur le fonctionnement de l'Union européenne précisent les compétences de l'Union dans les domaines de la coopération judiciaire en matière pénale, ainsi que de la protection des données et de la vie privée. Afin de*

préserver l'intégrité du droit de l'Union et de garantir la cohérence entre les dispositions du droit international et du droit de l'Union, il est nécessaire que l'Union participe aux négociations sur le deuxième protocole additionnel.» Les visas du préambule de la recommandation ne font toutefois pas référence à la base juridique matérielle de l'acte juridique.

23. Conformément à l'article 296, paragraphe 2, du TFUE et à la jurisprudence constante de la CJUE[35], 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.

24. **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 du protocole envisagé, parmi lesquels 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 afin de permettre le transfert des données à caractère personnel en toute légalité. De cette manière, le protocole envisagé serait directement en rapport avec les objectifs visés par l'article 16 du TFUE.

25. 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, point a), du TFUE*»[36].

4.2. Transferts ultérieurs

26. Relativement au transfert ultérieur par l'autorité de réception dans le pays tiers vers un autre pays tiers, le CEPD souligne que la CJUE a estimé, dans son avis 1/15 de juillet 2017, 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*». 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 [d'adéquation] de la Commission [...] couvrant les autorités vers lesquelles le transfert des données PNR est envisagé*»[37]. Par conséquent, **le CEPD recommande d'ajouter cette exigence supplémentaire aux directives de négociation.**

4.3. Droits des personnes concernées

27. Le CEPD prend note du fait que l'annexe n'inclut aucune directive spécifique concernant les droits des personnes concernées. 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. Le CEPD reconnaît que l'exercice des droits des personnes concernées est habituellement limité dans le contexte de la répression afin d'éviter de compromettre des enquêtes en cours. Néanmoins, dans son récent avis 1/15, il rappelle que la CJUE 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 [c]harte, un recours effectif devant un tribunal*»[38].

28. 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 au protocole envisagé veillent 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

29. 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.

30. Le CEPD rappelle que, conformément à la jurisprudence de la CJUE[39], 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*»[40].

31. Le CEPD remarque que ladite exigence ne traite pas spécifiquement des directives de négociation.

32. Le CEPD recommande que les directives de négociation visent à introduire dans le protocole un **mécanisme requérant de chaque pays partie du protocole qu'il mentionne clairement la ou les autorités spécifiques en charge** du contrôle indépendant du respect des règles du protocole envisagé. Le protocole 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 du protocole envisagé.

4.5. Recours juridictionnel et administratif

33. Le CEPD rappelle que la CJUE a conclu que[41] 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 que «*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*»[42].

34. En outre, la CJUE a souligné qu'il était essentiel que les personnes puissent introduire des plaintes auprès d'autorités de contrôle indépendantes[43] et demander à exercer, par conséquent, un recours administratif.

35. **Le CEPD recommande d'inclure dans le mandat l'objectif visant à assurer que le protocole garantisse la disponibilité des deux recours pour toutes les personnes concernées,** d'autant plus que toutes les parties à la convention sur la cybercriminalité ne tombent pas sous la juridiction de la Cour européenne des droits de l'homme.

4.6. Infractions pénales reprises par le protocole et catégories de données à caractère personnel

36. 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*»[44]. Lorsqu'il n'est pas possible de tirer de telles conclusions, et qu'on ne peut par conséquent *définir l'accès comme une ingérence grave dans les droits fondamentaux des personnes concernées*, la Cour a en outre conclu que «*l'ingérence que comporterait un accès à de telles données est donc susceptible d'être justifiée [...] 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"*»[45].

37. En ce qui concerne l'acquisition de connaissances des **données relatives au contenu**, il résulte de la jurisprudence de la CJUE qu'elle peut porter préjudice au contenu essentiel du droit à la vie privée[46].

38. 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*»[47] 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*»[48].

39. **Le CEPD souligne l'importance de définir de manière claire et directe les catégories de données concernées par le protocole envisagé afin de garantir la sécurité juridique** de toutes les parties prenantes concernées. 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[49], **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 du protocole.

40. 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 dans les directives de négociation que les distinctions devraient également se fonder sur la gravité des infractions concernées**. À cet égard, le **CEPD est en faveur de la définition d'une liste commune des infractions distinguant les différents degrés de gravité des infractions et pouvant varier en fonction du caractère restrictif des mesures prévues dans le protocole**.

4.7. Sécurité de l'information

41. Le CEPD considère que le protocole envisagé soulève des questions importantes concernant la sécurité de la transmission transfrontalière entrante et sortante de données à caractère personnel. Le CEPD souhaite souligner que garantir la sécurité des données à caractère personnel est non seulement une exigence claire du droit de l'Union[50], 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.

42. Par conséquent, **le CEPD recommande d'inclure dans le mandat des garanties supplémentaires concernant la vie privée et la protection des données en vue d'assurer un niveau de sécurité approprié aux données à caractère personnel produites et transférées. En outre, 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**.

4.8. Privilèges et immunités

43. Le CEPD recommande que le protocole, en sus d'inclure des garanties adaptées relatives à la protection des données à caractère personnel, veille au respect d'autres garanties liées aux données en tant que privilèges et immunités.

4.9. Urgence et assistance mutuelle[51]

44. Conformément au **point g),** l'Union européenne devrait appuyer le projet de texte et de rapport explicatif préliminaire adopté. En outre, le champ de l'assistance mutuelle devrait être semblable à celui défini à l'article 25 de la convention sur la cybercriminalité. En l'absence de toute référence croisée à une version spécifique du projet, le CEPD fonde ses commentaires sur le projet provisoire du 28 novembre 2018, disponible en ligne sur le site web du Conseil de l'Europe[52]. **Le CEPD recommande de prévoir la possibilité de concilier les objectifs de lutte contre le crime et le respect des droits fondamentaux en veillant à ce que le protocole permette à la partie requérante d'imposer des**

garanties et conditions spécifiques pour le transfert et de refuser une assistance pour des raisons de protection des données[53].

4.10. Collaboration directe entre les autorités répressives et les prestataires de services

a) Conditions spécifiques conformes au droit de l'Union pour le transfert de données à caractère personnel par les autorités répressives des États membres directement aux prestataires de services établis dans des pays tiers

45. 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[54], 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 en vertu de l'article 39 de la directive en matière de protection des données dans le domaine répressif[55], et uniquement si certaines conditions supplémentaires[56] sont remplies. Parmi ces conditions particulières figurent, 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[57]. **Le CEPD considère que le protocole envisagé 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.**

b) Définitions et types de données

46. Selon la recommandation, la disposition envisagée concernerait les informations de l'abonné[58]. Le CEPD salue le **point k)** établissant que le protocole devrait inclure des «*garanties appropriées en matière de droits fondamentaux, tenant compte des différents degrés de sensibilité des catégories de données concernées et des garanties prévues dans les injonctions européennes de production pour les différentes catégories de données*».

47. Le protocole pourrait être l'occasion de définir plus en détail les catégories de données afin de simplifier la mise en œuvre de la convention, en tenant compte des résultats des négociations sur la proposition relative aux preuves électroniques, le cas échéant. **À cet égard, le CEPD souligne l'importance de définir de manière claire et directe les catégories de données concernées par le protocole envisagé afin de garantir la sécurité juridique de toutes les parties prenantes associées à l'Union et les pays tiers contractants**. 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 devrait se limiter aux graves délits uniquement (voir section 4.6 ci-dessus).

c) Participation des autorités judiciaires dans d'autres pays parties au protocole

48. En ce qui concerne le **point l) de l'annexe**[59], le CEPD souligne qu'il semble prématuré de considérer les garanties consistant en «*une notification ou une approbation par l'État du fournisseur de services et un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante*» comme complémentaire de la proposition relative aux preuves électroniques, étant donné que cette dernière est toujours en cours de négociation. Le CEPD **recommande une approche plus prudente en prévoyant dans l'annexe des directives visant à soutenir des garanties supplémentaires et motifs de refus pertinents par rapport au droit secondaire de l'Union sur la collecte de preuves électroniques dans des affaires pénales, nécessaires pour assurer le niveau adapté de garanties, en particulier en ce qui concerne la protection des données à caractère personnel et la vie privée.**

49. En particulier, même dans le cadre de l'Union, dans son avis sur la proposition relative aux preuves électroniques, le comité européen de la protection des données, duquel est membre le CEPD, ne voit «*aucune justification à la procédure prévue dans le projet de règlement concernant les preuves électroniques permettant la production de données relatives au contenu sans la participation au moins des autorités compétentes de l'État membre dans lequel se trouve la personne concernée*»[60]. Au sein du Conseil, aucune notification aux autorités de l'État membre où se trouve la personne concernée n'a été introduite.

50. En outre, 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*»[61]. Au sein du Conseil, plusieurs États membres ont demandé de plus amples pouvoirs à l'autorité notifiée, au-delà de la notification introduite dans l'orientation générale et couvrant également les données non relatives au contenu[62].

51. Selon l'approche traditionnelle en matière d'accès transfrontière aux preuves électroniques, il incombe prioritairement au pays d'exécution de garantir le contrôle de motifs de refus limités. Bien que le CEPD 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 pays parties au protocole, notamment celles portant sur la recevabilité des preuves collectées dans un autre pays et sur ce qui constitue une infraction pénale, peuvent diverger. 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[63]. 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.

52. Les États membres ont l'obligation légale de respecter les droits fondamentaux lors de la mise en œuvre du droit de l'Union[64]. À cet égard, dans le contexte des négociations relatives à la directive concernant la décision d'enquête européenne[65], 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***»[66].

53. **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 s'agit également de garanties complémentaires dans les cas où la personne concernée ne peut être localisée ou est localisée dans un pays tiers qui ne constitue pas partie au protocole. **Il recommande par conséquent d'inclure dans les directives de négociation, en tant que garantie spécifique, l'obligation pour les autorités compétentes des pays parties au protocole 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**. 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)[67].

d) Possibilité pour les fournisseurs de services de s'opposer à une injonction

54. Les fournisseurs de services qui reçoivent une injonction relative à l'obtention de preuves électroniques adressée par les autorités compétentes d'un pays tiers partie au protocole pourraient se trouver pris entre des obligations légales contradictoires, l'une relevant du droit de l'Union et l'autre du droit du pays tiers. Le CEPD salue le **point c)** des directives de négociation, qui prévoit que le protocole prévienne les conflits de lois.

55. 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 le protocole envisagé, tels que des informations manquantes ou inexactes, ou des considérations relatives aux droits fondamentaux[68]. 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, **le CEPD recommande de préciser dans les directives de négociation que le protocole devrait prévoir un mécanisme conférant à un prestataire de services le droit de s'opposer à une injonction sur le fondement de motifs spécifiques définis aux présentes**.

4.11. Suspension du protocole en raison d'une violation du protocole par un pays et réexamen

56. Le CEPD note que la **section 3** de l'annexe prévoit la possibilité de dénoncer le protocole ainsi que les dispositions de la convention sur la cybercriminalité. Comme pour les décisions constatant le caractère adéquat conformément à l'article 45 du RGPD et l'article 36, paragraphe 5, de la directive relative à la protection des données dans le domaine répressif, le **CEPD considère qu'il est plus qu'important de prévoir, dans les**

directives de négociation, une clause permettant la suspension du protocole avec un pays tiers en cas de violations de ses dispositions par ledit pays.

57. De même, **le CEPD recommande que les directives de négociation prévoient la demande d'introduction d'une clause définissant un réexamen périodique obligatoire du fonctionnement pratique du protocole**. Afin de garantir un réexamen révélateur, celui-ci doit être prévu au plus tard un an après l'entrée en vigueur du protocole, puis à intervalles réguliers. Il convient également de préciser la fréquence de ces réexamens complémentaires. Le contenu du réexamen devrait être précisé. Le réexamen devrait se concentrer non seulement sur la mise en œuvre du protocole, mais également sur l'évaluation de sa nécessité et proportionnalité. Aux fins d'un tel réexamen, il conviendrait de prévoir une coopération des parties contractantes avec le T-CY en matière de collecte d'informations, en ce compris les statistiques et la jurisprudence, concernant le fonctionnement pratique de la convention. Les équipes en charge du réexamen devraient se composer d'experts en protection des données et faire participer les autorités de protection des données à caractère personnel de l'Union.

5. CONCLUSIONS

58. Le CEPD comprend que les autorités répressives doivent pouvoir recueillir et obtenir des preuves électroniques rapidement et efficacement. Il est en faveur de l'utilisation d'approches innovantes pour obtenir un accès transfrontalier aux preuves électroniques et trouver une réponse aux interrogations actuelles à ce sujet. Un deuxième protocole additionnel négocié à l'échelle de l'Union 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'accords distincts conclus bilatéralement par les États membres. 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 du Conseil de participer aux négociations relatives au protocole.

59. Le CEPD salue le fait que l'objectif du mandat est de veiller à ce que le protocole prévoit des garanties appropriées pour la protection des données.

60. Le CEPD émet trois recommandations principales pour que le protocole envisagé garantisse le respect de la charge et de l'article 16 du TFUE. Il recommande que les directives de négociation visent à:
    - garantir le caractère obligatoire du protocole envisagé,
    - introduire des garanties détaillées – en ce compris le principe de limitation des finalités – étant donné la multitude de signataires potentiels, tous ne constituant pas parties à la convention 108 ou n'ayant pas conclu d'accord équivalent à l'accord-cadre UE-US,
    - s'opposer à toutes dispositions sur l'accès direct aux données.

61. Outre ces recommandations générales, les recommandations et observations formulées par le CEPD dans le présent avis portent sur les aspects spécifiques suivants:

    - la base juridique de la décision du Conseil;

- les transferts ultérieurs par les autorités compétentes des pays tiers;
- les droits des personnes concernées, notamment le droit d'être informé et le droit d'accès;
- le contrôle par une autorité indépendante;
- le recours juridictionnel et administratif;
- les infractions pénales définies par le protocole envisagé et les catégories de données à caractère personnel;
- les garanties spécifiques destinées à assurer un niveau approprié de sécurité des données transférées;
- les garanties spécifiques pour les données protégées par des privilèges et immunités;
- l'assistance mutuelle d'urgence;
- en cas de coopération directe, le transfert de données à caractère personnel, la définition et les types de données, la participation d'autres autorités, la possibilité pour les prestataires de services ayant reçu une injonction de soumettre des preuves électroniques de s'opposer sur la base de motifs spécifiques;
- la possibilité de suspendre le protocole en cas de manquements aux dispositions et de le réviser.

62. 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 ultérieurement consulté à propos des dispositions du projet de protocole 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 du 4.5.2016, p. 89 (ci-après la «directive relative à la protection des données dans le domaine répressif»).
[4] 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.
[9] Avis 2/2019 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.
[10] Convention sur la coopération internationale renforcée sur la cybercriminalité et les preuves électroniques, Budapest, 23 novembre 2001, SCTE nº 185.
[11] Voir état des signatures et ratifications relatif à la convention sur la cybercriminalité pour une liste exhaustive et actualisée des pays parties à la convention sur la cybercriminalité, disponible sur: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ZZawh58m
[12] Note d'observation nº 3 intitulée «Accès transfrontalier aux données (article 32)» du T-CY, T-CY (2013)7 E, p. 3, disponible sur:
https://rm.coe.int/16802e726a
[13] Voir page web du Conseil de l'Europe à l'adresse suivante: https://rm.coe.int/t-cy-pd-f-pubsummary-v6-mar2018-/1680795712.
[14] Ceci concerne les cas pour lesquels les autorités peuvent directement demander à un prestataire de services d'une autre juridiction de conserver et de produire des données.
[15] Ceci concerne les cas pour lesquels les autorités peuvent elles-mêmes directement accéder aux données transfrontalières, sans l'intervention d'un intermédiaire.
[16] Mandat pour la préparation d'un projet de 2e protocole additionnel à la convention de Budapest sur la cybercriminalité, juin 2017, disponible à l'adresse suivante: https://rm.coe.int/mandat-pour-la-preparation-d-un-projet-de-2e-protocole-a-la-convention/168072380f.
[17] Voir fiche d'information de la Commission européenne disponible sur: http://europa.eu/rapid/press-release_MEMO-19-865_fr.htm.
[18] Soulignement ajouté.
[19] Voir doc. prél. nº 10 de décembre 2008 – Le caractère obligatoire ou non obligatoire de la convention preuves [en matière civile ou commerciale]: https://assets.hcch.net/upload/wop/2008pd10e.pdf.
[20] p. 7.
[21] Affaires jointes C-402/05 P et C-415/05 P, Kadi/Conseil, ECLI:EU:C:2008:461, point 285. [Soulignement ajouté].
[22] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 95.
[23] Voir en particulier les points b), c), m) et o) de l'annexe.
[24] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592.
[25] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 214, voir également le point 93.
[26] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, STE nº 108 (ci-après la «convention 108»).
[27] Voir à ce sujet, p. 6 de l'avis 4/2001 du GT art. 29 concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité, adopté le 22 mars 2001 (5001/01/FR/Final WP 41): «les signataires devraient être invités à signer la convention 108 du Conseil de l'Europe».

[28]Il semble notamment que tous les pays tiers parties à la convention sur la cybercriminalité ne sont pas parties à la convention 108 ou à la convention européenne des droits de l'homme, et que certains d'entre eux sont parties à la convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel. Le protocole modifiant la convention 108, la «convention 108+», n'est pas encore entré en vigueur. Il a été signé par de nombreux États membres mais n'a pas encore été ratifié – voir état des signatures et ratifications de ladite convention: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223/signatures.

[29] Exposé des motifs, p. 6.

[30] Document de travail des services de la Commission: Analyse d'impact, SWD(2018) 118 final (ci-après «analyse d'impact sur la proposition relative aux preuves électroniques»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=SWD%3A2018%3A118%3AFIN, p. 33: «Accès étendu, c.-à-d. l'utilisation du dispositif d'un suspect ou d'un témoin saisi dans le cadre d'une enquête (p. ex., à l'aide d'un mandat de perquisition et de saisie) afin d'accéder aux données accessibles à partir de l'appareil (en ce compris le nuage). La plupart des États membres permettent à leurs pouvoirs publics de mener ce genre d'accès direct».

[31] Exposé des motifs, p. 6.

[32] Analyse d'impact sur la proposition relative aux preuves électroniques, p. 11: «la législation nationale d'au moins 20 États membres autorise les autorités détenant une autorisation judiciaire à saisir et à rechercher un appareil et à enregistrer à distance les données accessibles à partir de celui-ci, ou à utiliser les identifiants d'un compte pour trouver et chercher des données stockées sur ce compte. Cet outil devient plus pertinent aujourd'hui en raison de l'enregistrement plus fréquent des informations sur des serveurs à distance, possiblement hors de l'État membre concerné ou même hors de l'Union européenne, plutôt que sur des dispositifs locaux.
Souvent, la localisation de ces données n'est pas connue des autorités répressives (ce que l'on appelle la "perte de connaissance de la localisation des données"), et il peut s'avérer quasiment impossible de la déterminer, comme dans les cas où les données sont hébergées sur des services du darknet qui utilisent de multiples couches de relais IP pour dissimuler leur localisation. Il peut donc s'avérer difficile de déterminer si de telles recherches ont une composante transfrontalière.
Les États membres ont différentes approches à l'accès direct et à la localisation des données».

[33] Commentaires du 5 décembre 2013, disponibles à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.
Le groupe de travail «article 29» a «attiré l'attention sur les risques liés à l'adoption d'un éventuel protocole additionnel qui légitimerait un accès direct des autorités répressives d'une partie à des données stockées dans la juridiction d'une autre partie. Le groupe de travail "article 29" souligne que l'application d'un tel principe, indépendamment de la façon dont il est mis en œuvre (p. ex., en appliquant la loi ou les définitions de consentement de la partie effectuant les recherches), violerait les règles de protection des données à caractère personnel et aurait des répercussions négatives sur les droits fondamentaux des particuliers». Et d'ajouter: «Un protocole additionnel à une convention internationale qui semblerait fournir un accès à des données stockées sur des ordinateurs à l'étranger conformément à la loi (ou à la définition du consentement) de la partie à l'origine des recherches enfreindrait l'acquis de l'Union relatif à la protection des données.» Il insistait également sur le fait que «les transferts des données transfrontières dans le domaine de la répression doivent exclure l'accès transfrontalier général/massif aux données ainsi que la collecte ou le transfert général(e) ou de masse de données, incompatibles avec la charte des droits fondamentaux de l'Union et la convention européenne des droits de l'homme».

[34] p. 6.

[35] Voir arrêt de la CJUE du 25 octobre 2017, Commission/Conseil (CMR-15), C-687/15, ECLI:EU:C:2017:803, point 48 et suivants.

[36] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 232.

[37] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 214.

[38] Avis 1/15, accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, point 220. [Soulignement ajouté].

[39] 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.

[40] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 230.

[41] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 95.

[42] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, point 95. [Soulignement ajouté].

[43] Arrêt de la CJUE du 6 octobre 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, points 56 à 58.

[44] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, point 54, voir également point 56.
[45] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, point 62. [Soulignement ajouté].
[46] 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.
[47] 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.
[48] 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.
[49] Voir 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-dessous l'«avis 23/2018 du comité européen de la protection des données»), disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2018-09-26-eevidence_fr.pdf, p. 14: «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».
[50] Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite 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.
[51] Selon le point 2 de la page 6 du projet de rapport explicatif, «[les] urgences supposant un risque important et imminent pour la vie ou la sécurité d'une personne concernent souvent des prises d'otages au cours desquelles il existe un réel risque de décès imminent, de blessures sérieuses ou de tout autre dommage à la victime, et le suspect négocie une rançon par courrier électronique ou au moyen des réseaux sociaux de telle sorte que la localisation de la victime peut être déterminée grâce aux données stockées par le fournisseur, des violences sexuelles à l'encontre d'un enfant mises en évidence par la découverte de matériel d'exploitation sexuelle d'enfants ou d'abus sexuels concernant des enfants, ou d'autres indices d'abus, des scénarios post-attentats lorsque les autorités cherchent à déterminer avec qui les terroristes communiquaient afin de savoir si d'autres attaques sont imminentes, et des menaces à la sécurité d'infrastructures critiques au sein desquelles il existe un risque de danger important et imminent à la vie ou à la sécurité de personnes physiques».
[52] https://rm.coe.int/t-cy-2018-23rev-protoprov-pub-text-v4/16808ff490
[53] Voir avis 4/2001 du GP art. 29 concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité, adopté le 22 mars 2001 (5001/01/FR/Final WP 41), p. 5 et suivantes.
Voir également étude «Les règles de procédure pénale dans l'Union européenne – Analyse comparative de quelques-unes des principales différences et de leurs incidences sur l'élaboration de la législation européenne» commanditée par le département thématique des droits des citoyens et des affaires constitutionnelles du Parlement européen, PE 604.977, p. 30.
Voir enfin avis délivré le 14 février 2011 par l'Agence des droits fondamentaux relativement au projet de directive concernant la décision d'enquête européenne, p 11: *«[un] motif de rejet fondé sur les droits fondamentaux pourrait constituer un outil adéquat pour prévenir les violations des droits fondamentaux dans le cadre d'enquêtes transfrontalières. Parallèlement, l'État d'exécution devrait connaître les règles et procédures pénales de l'État d'émission, ainsi que les détails de l'affaire concernée. Par conséquent, une véritable évaluation des droits fondamentaux dans chaque affaire n'irait pas uniquement à l'encontre de l'idée de reconnaissance mutuelle, mais en raison des procédures complexes et longues, pourrait également porter préjudice à certaines normes relatives aux droits fondamentaux définies à la section 2.2. Pour cette raison, toute définition d'un motif de rejet reposant sur les droits fondamentaux dans la directive devrait idéalement être complétée par des paramètres explicites. De tels paramètres pourraient limiter le motif de refus aux circonstances dans le cadre desquelles un État membre de l'Union craint, à juste titre, que l'exécution d'une décision d'enquête européenne entraîne une violation des droits fondamentaux de la personne concernée. Ainsi, un motif de refus reposant sur des droits fondamentaux pourrait servir en tant que "valve de sécurité", facilitant le respect des États membres des obligations relatives aux droits fondamentaux découlant du droit primaire de l'Union sans que les États membres n'aient à s'écarter du droit secondaire de l'Union».*
[54] 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.

[55] Il s'agit d'une dérogation spécifique 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.

[56] 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».

[57] Voir avis 23/2018 du comité européen de la protection des données, p. 9.

[58] Les informations des abonnés sont définies à l'article 18, paragraphe 3, de la convention: «toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service». Voir également rapport explicatif de la convention sur la cybercriminalité, point 177 et suivants.

[59] Le point (l) établit ce qui suit: «S'agissant de ces dispositions, l'Union européenne ne devrait pas s'opposer à l'ajout dans le deuxième protocole additionnel de garanties et motifs de refus par rapport aux propositions de la Commission relatives aux preuves électroniques, y compris à mesure qu'elles évoluent au cours des négociations entre les colégislateurs dans le cadre de la procédure législative et finalement sous leur forme définitive (adoptée): par exemple, lesdites dispositions pourraient prévoir une notification ou une approbation par l'État du fournisseur de services et un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, tant que cela ne réduit pas de manière disproportionnée l'efficacité de l'instrument prévu dans le deuxième protocole additionnel (par exemple, dans des cas d'urgence dûment justifiés). Les garanties ou motifs de refus supplémentaires ne devraient pas affecter le fonctionnement des propositions de l'UE relatives aux preuves électroniques entre les États membres».

[60] Voir avis 23/2018 du comité européen de la protection des données, p. 16.

[61] Voir avis 23/2018 du comité européen de la protection des données, p. 17.

[62] 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*».

[63] Voir liste de motifs d'objection mentionnés à l'article 14 de la proposition relative aux preuves électroniques, ainsi que la jurisprudence développée par la CJUE dans le contexte 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).

[64] Voir article 6 du traité sur l'Union européenne et l'article 67, paragraphe 1, du TFUE. Voir également avis délivré le 14 février 2011 par l'Agence des droits fondamentaux relativement 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 c. Irlande, nº 45036/98, 30 juin 2005, point 156: «il y a lieu de présumer qu'un État respecte les exigences de la Convention 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».

[65] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

[66] Voir avis délivré le 14 février 2011 par l'Agence des droits fondamentaux relativement au projet de directive concernant la décision d'enquête européenne, note 61 faisant référence à l'arrêt nº 30696/09 de la CEDH du 21 janvier 2011, M.S.S. c. Belgique et Grèce.

[67] Voir considérant 6 de la recommandation.

[68] Voir page 17 de l'avis 23/2018 du comité européen de la protection des données dans lequel le comité recommande que la proposition relative aux preuves électroniques «*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*».