EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

20 janvier 2022

Avis 1/2022

concernant les deux propositions de décisions du Conseil autorisant les États membres à signer et à ratifier, dans l'intérêt de l'Union européenne, le deuxième Protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

edps.europa.eu

Le Contrôleur européen de la protection des données («CEPD») est une institution indépendante de l'Union européenne 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».

Wojciech Rafał Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

*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 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, notamment lors de la négociation d'accords avec des pays tiers dans le secteur de l'application de la loi. Il s'appuie sur l'obligation générale exigeant que les accords internationaux 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'UE. En particulier, il convient de veiller au respect des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne ainsi que de l'article 16 TFUE.

Résumé

Le 25 novembre 2021, la Commission a adopté deux propositions de décisions du Conseil, au titre de l'article 16, de l'article 82, paragraphe 1, et de l'article 218, paragraphes 5 et 6, du traité sur le fonctionnement de l'Union européenne, l'une autorisant les États membres à signer et l'autre à ratifier, dans l'intérêt de l'Union européenne, le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité. L'annexe des propositions contient les instructions du Conseil concernant les réserves, les déclarations et les communications lors de la signature et de la ratification du protocole.

Les enquêtes et les poursuites pénales sont un objectif légitime, et la coopération internationale, y compris l'échange d'informations, est devenue plus importante que jamais. 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 sous forme électronique dans un pays tiers. Le volume croissant de demandes et le caractère volatil des informations numériques mettent 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 visant à concevoir de nouveaux modèles de coopération, y compris dans le cadre de la coopération avec les pays tiers.

Le protocole vise à améliorer les canaux de coopération traditionnels et comprend des dispositions visant à renforcer la coopération directe entre les autorités répressives et les fournisseurs de services dans un contexte transfrontière. En particulier, le protocole renforcerait la coopération en matière de cybercriminalité et la collecte de preuves sous forme électronique concernant des infractions pénales aux fins d'enquêtes ou de procédures pénales spécifiques.

Tout en reconnaissant qu'il n'est pas possible de reproduire entièrement la terminologie et les définitions du droit de l'UE dans un accord international multilatéral, le CEPD souligne que les garanties appropriées pour les personnes doivent être prévues afin de respecter pleinement le droit de l'Union.

Les principes de protection des données, notamment l'équité, l'exactitude et la pertinence des informations, le contrôle indépendant et les droits individuels des personnes physiques, sont aussi pertinents pour les organismes publics que pour les entreprises privées. Ces principes de base sont d'autant plus importants que les données nécessaires aux enquêtes pénales sont sensibles.

Le présent avis vise à fournir une analyse objective et des conseils constructifs aux institutions de l'UE, alors que le Conseil examine les propositions de la Commission visant à signer et à ratifier le protocole et avant que le Parlement européen ne soit appelé à donner son accord à la conclusion du protocole.

Le CEPD se félicite qu'aucune disposition relative à l'accès direct des autorités répressives aux données n'ait été incluse dans le texte final du protocole. Il se réjouit également du fait que le protocole contienne un article consacré à la protection des données à caractère personnel. En outre, le CEPD prend note avec satisfaction des nombreuses garanties qui ont été incluses dans le protocole.

Le CEPD comprend qu'il est confirmé que l'accord-cadre UE-États-Unis s'appliquerait aux transferts de l'UE vers les États-Unis d'Amérique dans le cadre des dispositions énoncées dans le protocole concernant la coopération entre les autorités. Le CEPD déplore ce résultat.

En cas d'adoption d'une décision du Conseil autorisant les États membres à, respectivement, signer et ratifier, dans l'intérêt de l'Union, le protocole, le CEPD se félicite des propositions de la Commission visant à ce que les États membres fassent, dans l'intérêt de l'Union, la déclaration, la notification et la communication au titre de l'article 7, paragraphe 2, point b), et de l'article 7, paragraphe 5, points a) et e), du protocole. Ces propositions garantissent que les fournisseurs de services de l'Union ne puissent être sollicités pour le transfert de données à caractère personnel que sur la base d'injonctions émises, dans le pays tiers requérant partie au Protocole, par un procureur ou une autre autorité judiciaire, ou sous la supervision d'un procureur ou d'une autre autorité judiciaire, ou sous une autre forme de supervision indépendante et sous le contrôle d'une autorité compétente dans l'État membre requis.

Le CEPD note également avec satisfaction la proposition selon laquelle les États membres font la déclaration visée à l'article 8, paragraphe 4, du protocole (sur la coopération entre les autorités compétentes pour donner suite aux injonctions de fournir les données relatives aux abonnés et au trafic), de sorte que des informations complémentaires soient nécessaires pour donner effet aux injonctions au titre de cette disposition.

En outre, le CEPD formule les recommandations suivantes en ce qui concerne les futures décisions du Conseil, si le protocole devait être signé et ratifié par les États membres, dans l'intérêt de l'Union:

- certaines données figurant dans la catégorie des informations relatives aux abonnés au sens de la convention sur la cybercriminalité peuvent être considérées, en vertu du droit de l'Union, comme des données relatives au trafic impliquant une ingérence grave dans les droits fondamentaux de la personne concernée, dont l'accès ne peut être justifié que par la lutte contre la criminalité grave. Par conséquent, contrairement à la proposition de la Commission, le CEPD recommande aux États membres de se réserver le droit de ne pas appliquer l'article 7 du protocole sur la divulgation des données relatives aux abonnés par les fournisseurs de services directement aux autorités compétentes d'un autre pays en ce qui concerne certains types de numéros d'accès, conformément à l'article 7, paragraphe 9, point b);

- les États membres devraient désigner, conformément à l'article 7, paragraphe 5, point e), du protocole, une autorité judiciaire ou une autre autorité indépendante;

- la communication proposée par les États membres aux autorités des États-Unis, au moment de la signature ou du dépôt de leur instrument de ratification, d'acceptation ou d'approbation, en rapport avec l'accord-cadre UE-États-Unis, devrait être clarifiée;

- il y a lieu de modifier l'examen proposé à l'aune d'autres accords ou arrangements au titre de l'article 14, paragraphe 1, point c), du protocole, qui pourraient remplacer sa disposition relative à la protection des données (article 14)

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 (ci-après la «Charte»), 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[2], et notamment son article 42, paragraphe 1, son article 57, paragraphe 1, point g), et son article 58, paragraphe 3, point c),

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. En juin 2017, le comité de la convention sur la cybercriminalité du Conseil de l'Europe a approuvé le mandat en vue de la préparation d'un deuxième protocole additionnel à la convention sur la cybercriminalité au cours de la période comprise entre septembre 2017 et décembre 2019[4].

2. Le 5 février 2019, la Commission a adopté une recommandation[5] de décision du Conseil visant à autoriser la participation de la Commission, au nom de l'Union européenne, aux négociations relatives à un deuxième protocole additionnel (ci-après le «protocole»)[6] à la convention du Conseil de l'Europe sur la coopération internationale renforcée en matière de cybercriminalité et de preuves électroniques (ci-après la «convention sur la cybercriminalité») (STCE nº 185)[7].

3. Le Contrôleur européen de la protection des données (ci-après le «CEPD») a adopté un avis sur la recommandation le 2 avril 2019[8]. Par décision du 6 juin 2019, le Conseil de l'Union européenne a autorisé la Commission à participer, au nom de l'Union européenne, aux négociations sur le protocole[9].

4. Le comité de la convention sur la cybercriminalité a prorogé le mandat à deux reprises, jusqu'en décembre 2020 dans un premier temps et jusqu'en mai 2021 ensuite. Le protocole a été élaboré par le comité de la convention sur la cybercriminalité (T-CY) entre septembre 2017 et mai 2021. Au cours de cette période, plus de quatre-vingt-dix sessions de la plénière de rédaction du protocole T-CY, du groupe de rédaction et des sous-groupes ainsi que six cycles de consultation des parties prenantes ont eu lieu.

5. Le comité européen de la protection des données (ci-après l'«EDPB») a contribué aux consultations publiques sur le projet de protocole le 13 novembre 2019, le 2 février 2021 et le 4 mai 2021[10].

6. Le Parlement européen a reconnu la nécessité de conclure les travaux sur le protocole dans sa résolution de 2021 sur la stratégie de cybersécurité de l'Union pour la décennie numérique[11].

7. Le 17 novembre 2021, le Comité des Ministres du Conseil de l'Europe a adopté le protocole. Il devrait être ouvert à la signature en mai 2022. Des amendements ne peuvent donc être proposés que par une partie au protocole et adoptés par le Comité des Ministres. Le protocole exige l'acceptation de toutes les parties pour que les amendements entrent en vigueur[12].

8. L'Union européenne ne peut devenir partie au protocole, étant donné que tant le protocole que la convention sur la cybercriminalité sont ouverts aux seuls États[13].

9. Le 25 novembre 2021, la Commission a adopté deux propositions de décisions du Conseil, au titre de l'article 16, de l'article 82, paragraphe 1, et de l'article 218, paragraphes 5 et 6, du traité sur le fonctionnement de l'Union européenne (ci-après le «TFUE»)[14].

10. Selon ces propositions[15], le protocole relève d'un domaine couvert, dans une large mesure, par des règles communes au sens de l'article 3, paragraphe 2, TFUE. Par ces propositions, la Commission cherche à obtenir deux décisions du Conseil autorisant les États membres à signer et à ratifier, respectivement, le protocole dans l'intérêt de l'Union européenne. Les deux propositions sont accompagnées d'une annexe (ci-après l'«annexe») qui donne des instructions aux États membres en ce qui concerne les réserves, déclarations, notifications ou communications et autres considérations à formuler lors de la signature et de la ratification, dans l'intérêt de l'Union européenne, du protocole. La proposition relative à la ratification est également accompagnée d'une annexe contenant le texte du protocole.

11. Pour que l'accord puisse être conclu, dans l'hypothèse ou le Conseil déciderait d'autoriser sa signature par les États membres, dans l'intérêt de l'Union, il devrait adopter une décision autorisant les États membres, dans l'intérêt de l'Union, à ratifier l'accord, après avoir obtenu l'approbation du Parlement européen. Le protocole entrera en vigueur le premier jour du mois suivant l'expiration d'une période de trois mois après la date à laquelle cinq parties à la convention sur la cybercriminalité auront exprimé leur consentement à être liées par le protocole, conformément aux dispositions de l'article 16, paragraphes 1 et 2, du protocole[16].

12. Le CEPD a été consulté sur les deux propositions par la Commission européenne après leur adoption, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725. Les considérants 12 et 13 des propositions relatives à la ratification et à la signature du protocole font référence au présent avis. Le CEPD tient à souligner que le présent avis est délivré sans préjudice des observations supplémentaires qu'il pourrait formuler sur la base d'informations disponibles ultérieurement.

2. Objectifs du deuxième protocole additionnel

13. La convention sur la cybercriminalité est ouverte aux États membres du Conseil de l'Europe et aux non-membres (sur invitation). À l'heure actuelle, 66 pays sont parties à la convention, en ce compris 26 États membres de l'Union (ci-après les «États membres»)[17] et d'autres pays tiers membres du Conseil de l'Europe comme l'Arménie, l'Azerbaïdjan et 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[18].

14. La convention sur la cybercriminalité est un instrument international contraignant requérant des parties qu'elles définissent des infractions pénales spécifiques commises à l'encontre de réseaux électroniques ou au moyen desdits réseaux dans leur législation nationale et établissent des pouvoirs et procédures spécifiques autorisant leurs autorités nationales à mener leurs enquêtes pénales, notamment en collectant des preuves électroniques. La convention comporte des exigences minimales concernant les pouvoirs d'enquête disponibles dans le cadre d'une enquête pénale et encourage la coopération internationale entre les parties. En particulier, son chapitre III sur la coopération internationale[19] contient à la fois des dispositions générales sur la coopération internationale, qui figurent également dans d'autres traités relatifs à la coopération en matière pénale, et des dispositions spécifiques à la collecte de preuves électroniques.

15. Le protocole vise à fournir des outils supplémentaires, y compris pour la coopération dans les situations d'urgence, comme expliqué plus en détail ci-dessous. Le protocole est accompagné d'un rapport explicatif[20] qui reflète l'interprétation des rédacteurs. Bien qu'il ne constitue pas un instrument fournissant une interprétation faisant autorité du protocole, il est destiné à «guider et aider les Parties» dans l'application du protocole[21].

16. Le protocole comprend:

    - des dispositions **permettant une coopération directe entre les autorités compétentes** d'une Partie, d'une part, et les entités fournissant **des services d'enregistrement de noms de domaine ou des fournisseurs de services** dans une autre partie, d'autre part, pour la divulgation, respectivement, de **données relatives à l'enregistrement de noms de domaines ou d'informations sur les abonnés**[22] (articles 6 et 7);

    - des dispositions **renforçant la coopération internationale entre les autorités**:

        - donner effet aux **injonctions ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic**[23] (article 8);

        - **les demandes non contraignantes** de **divulgation accélérée de données informatiques stockées**[24] **en cas d'urgence** (article 9);

        - **l'entraide judiciaire d'urgence** (article 10)[25];

        - la vidéoconférence (article 11);

    - les enquêtes communes et les équipes communes d'enquête (article 12);

    - **des conditions et garanties** (articles 13 et 14), **y compris les exigences en matière de protection des données**. Des conditions et garanties spécifiques sont également intégrées dans les mesures de coopération spécifiques.

17. Les demandes de coopération directe pour la divulgation de données relatives à l'enregistrement de noms de domaine (article 6) et les demandes de divulgation accélérée de données informatiques stockées en situation d'urgence (article 9) sont des demandes *non contraignantes*[26].

18. Le protocole prévoit **qu'une partie peut *se réserver le droit de ne pas appliquer***:

– l'article 7 (coopération directe pour la divulgation d'informations relatives aux abonnés) dans son intégralité ou, si la divulgation de certains types de numéros d'accès en vertu de cet article était incompatible avec les principes fondamentaux de son ordre juridique interne, de ne pas appliquer cet article à ces numéros (article 7, paragraphe 9)[27];

– l'article 8 (renforcement de la coopération internationale entre les autorités donnant effet aux injonctions ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic) aux données relatives au trafic (article 8, paragraphe 13)[28].

19. Le protocole prévoit également **la possibilité pour une partie *de faire certaines déclarations***, notamment les déclarations suivantes:

– au titre de l'article 7 (coopération directe pour la divulgation d'informations relatives aux abonnés), permettant à la partie requise d'exiger que, lorsqu'une injonction est adressée à un fournisseur de services sur son territoire:

  o cette injonction soit émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante [paragraphe 2, point b)];

  o la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure d'une autorité qui peut donner instruction aux fournisseurs de services de ne pas divulguer les informations relatives à l'abonné si certaines conditions ou motifs de refus sont remplis [paragraphe 5, points a) et e)];

– au titre de l'article 8 (production accélérée de données relatives aux informations sur les abonnés et au trafic), permettant à la partie requise de déclarer que des informations supplémentaires sont nécessaires pour donner effet à des injonctions (paragraphe 4).

20. Dans les propositions de décisions du Conseil, la Commission propose que les États membres soient autorisés à signer et à ratifier le protocole, en agissant conjointement dans l'intérêt de l'Union, avec un certain nombre de réserves et de déclarations. En particulier, **les États membres sont invités à s'abstenir de se réserver le droit de ne pas appliquer l'article 7 dans son ensemble** ou en ce qui concerne certains types de numéros d'accès[29] et sont encouragés à s'abstenir de se réserver le droit de ne pas appliquer l'article 8 (donnant effet à des injonctions concernant les données relatives aux informations sur les abonnés et au trafic provenant d'une autre partie) en ce qui concerne les données relatives au trafic conformément à l'article 8, paragraphe 13. La proposition de décision du Conseil **donne toutefois instruction aux États membres de se prévaloir des déclarations susmentionnées au titre des articles 7 et 8 afin que les garanties supplémentaires qui y figurent soient applicables**[30].

3. Observations générales

21. 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 visant à concevoir de nouveaux modèles de coopération, y compris dans le cadre de la coopération avec les pays tiers. À cet égard, il réitère son appel, conjointement avec le comité européen de la protection des

données, à mettre en œuvre une nouvelle génération de traités d'entraide judiciaire, ce qui permettra un traitement beaucoup plus rapide et sûr des demandes dans la pratique[31].

22. En vertu de l'article 216, paragraphe 2, TFUE, les accords internationaux conclus par l'Union «*lient les institutions de l'Union et les États membres*». En outre, selon la jurisprudence constante de la Cour de justice de l'Union européenne (ci-après la «CJUE»), les accords internationaux forment, à partir de leur entrée en vigueur, «*partie intégrante [...] de l'ordre juridique communautaire*»[32] et bénéficient de la primauté sur les actes de droit dérivé de l'Union[33].

23. Étant donné que la convention sur la cybercriminalité, à l'instar de ses différents protocoles additionnels, est un instrument international contraignant, le CEPD note que, conformément à la jurisprudence de la CJUE, «*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*»[34]. Il est donc essentiel de veiller à ce que les obligations découlant du protocole ne portent pas atteinte à ces principes en ce qui concerne la protection des données.

24. Le protocole que la Commission propose de signer et de ratifier autoriserait, entre autres, les transferts de données à caractère personnel provenant des autorités compétentes[35] des États membres et d'entités privées situées dans les États membres[36], ainsi que le traitement ultérieur de ces données par les autorités des pays tiers parties au protocole et par des entités privées de ces pays.

25. À cet égard, le considérant 8 des deux propositions indique qu'«*[é]tant donné que le protocole prévoit des garanties appropriées conformes aux exigences applicables aux transferts internationaux de données à caractère personnel au titre du règlement (UE) 2016/679 et de la directive (UE) 2016/680, son entrée en vigueur contribuera à promouvoir les normes de l'Union en matière de protection des données au niveau mondial, facilitera les flux de données entre les parties au protocole qui sont des États membres de l'UE et celles qui ne le sont pas et garantira le respect, par les États membres de l'UE, des obligations qui leur incombent en application des règles de l'Union relatives à la protection des données*».

3.1. Traitement, par une autorité d'un État membre ou une entité privée sur le territoire d'un État membre[37], de données à caractère personnel reçues au titre du protocole

26. L'article 14 du protocole concerne la protection des données à caractère personnel. Le paragraphe 1, point e), de cette disposition prévoit qu'aucune disposition de cet article «*n'empêche une Partie d'appliquer des garanties plus strictes au traitement par ses propres autorités des données à caractère personnel reçues en vertu du présent Protocole*». Les États membres seraient donc autorisés à appliquer des garanties plus strictes au traitement, par leurs autorités ou par une entité privée située sur leur territoire, des données à caractère personnel reçues en vertu du protocole.

3.2. Transferts vers des pays tiers parties au protocole

27. Le CEPD note qu'en vertu des articles 6 et 7, le protocole autorise les transferts de données à caractère personnel par des entités privées, dans un but répressif différent de celui pour lequel les données ont été collectées.

28. À titre liminaire, le CEPD relève que l'ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données garantis par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»), permise par le protocole, doit satisfaire aux exigences de l'article 52, paragraphe 1, de la Charte.

29. Les transferts d'une autorité répressive à un fournisseur de services ou à une entité fournissant des services d'enregistrement de noms de domaine dans un État tiers doivent respecter les principes de la protection des données énoncés dans la directive (UE) 2016/680[38], en particulier ceux prévus au chapitre V de la directive, afin de garantir que le niveau de protection des personnes physiques garanti par le droit de l'Union ne soit pas compromis.

30. Conformément à l'article 44 du règlement (UE) 2016/679 (ci-après le «RGPD»)[39], il convient d'apprécier si le protocole garantit que les transferts effectués par des entités privées dans le cadre des articles 6 et 7 dudit protocole peuvent avoir lieu dans les conditions énoncées au chapitre V du RGPD, sous réserve des autres dispositions du règlement (voir section 4).

31. En ce qui concerne le transfert, par des entités privées dans l'Union, de données requises par une décision d'une juridiction ou d'une autorité administrative d'un pays tiers, il découle de l'article 48 du RGPD que cette décision «*ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du [chapitre V]*» du RGPD.

32. En juillet 2017, dans son avis 1/15[40] concernant l'accord international sur le transfert de données des dossiers passagers («PNR») entre le Canada et l'UE, la CJUE précise les conditions dans lesquelles un accord international peut constituer une base juridique pour les transferts de données à caractère personnel relevant du champ d'application de la directive 95/46/CE (désormais remplacée par le RGPD). 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*»[41]. **Il ressort de l'avis 1/15 que le niveau de protection résultant du protocole pour l'échange de données à caractère personnel avec des pays tiers devrait être substantiellement équivalent au niveau de protection prévu par le droit de l'Union.** À cet égard, le CEPD souligne que, conformément à la jurisprudence de la CJUE, les articles 7 et 8 de la Charte doivent être appréciés conjointement au **droit à un recours effectif prévu à l'article 47 de la Charte**[42].

33. S'agissant de la base juridique, en vertu de l'article 6 du protocole, les demandes d'informations relatives à l'enregistrement de noms de domaine émises au titre du protocole constituent la base d'une coopération volontaire et ne sont donc pas contraignantes, en vertu du protocole, pour l'entité requise. Le protocole laisse aux parties le soin de déterminer les modalités de mise en œuvre[43]. En ce qui concerne les injonctions au titre de l'article 7, le protocole exige que les parties adoptent les mesures nécessaires pour que les fournisseurs de services établis sur leur territoire répondent à une injonction émise par une autorité compétente d'une autre partie. Le rapport explicatif indique à cet égard que «*[l]es modalités de sa mise en œuvre dépendent des considérations légales et politiques des différentes Parties*»[44].

34. Pour les États membres, il s'agirait notamment de définir, selon le rapport explicatif, «*une base claire pour le traitement des données à caractère personnel. Au vu des exigences supplémentaires prévues par les lois sur la protection des données pour autoriser d'éventuels transferts internationaux de données relatives aux abonnés, le présent Protocole traduit l'importance de l'intérêt public pour cette mesure de coopération directe et prévoit à son article 14 les garanties requises à cette fin*». Le RGPD prévoit une base juridique possible dans de tels cas[45] et le

Protocole n'empêche pas le droit national de préciser davantage la base juridique des transferts, tant qu'il permet la coopération prévue par le protocole[46].

4. Garanties concernant les transferts internationaux de données et le respect des droits fondamentaux

4.1. Statut du protocole en ce qui concerne la protection des données

35. Si tous les États membres sont parties à la convention 108[47] du Conseil de l'Europe, qui est applicable dans le domaine répressif, tous les pays tiers Parties à la convention sur la cybercriminalité ne sont pas parties à la convention 108[48]; seule une minorité bénéficie d'une décision d'adéquation au titre du RGPD[49] et un seul (le Royaume-Uni) bénéficie d'une décision d'adéquation au titre de la directive (UE) 2016/680.

36. Au vu 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 traiter et atténuer ces risques de manière satisfaisante.

37. L'**article 14** du protocole sur la protection des données à caractère personnel prévoit des garanties **en ce qui concerne les données reçues en vertu du protocole**, y compris les données reçues dans le cadre d'une injonction ou d'une demande au titre du Protocole, pour «permettre aux parties de satisfaire à ces obligations [en matière de protection des données]» en ce qui concerne les transferts de données à caractère personnel aux fins du protocole[50]. À cet égard, le CEPD note avec satisfaction que la notion de données à caractère personnel, telle que définie à l'article 3 du protocole est conforme au protocole d'amendement à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE 223) (convention 108+) et au droit de l'Union.

38. Il appartiendrait aux autorités répressives des États membres d'évaluer la proportionnalité de leurs demandes ou injonctions au titre du protocole[51]. De même, il appartiendrait à ces autorités d'évaluer si leurs demandes ou injonctions de produire des données à caractère personnel à un pays tiers partie au protocole sont conformes aux exigences du droit de l'Union avant d'envoyer une demande ou une injonction.

39. Conformément à l'article 14, paragraphe 1, point d), «*chaque Partie considère que le traitement des données à caractère personnel conformément aux paragraphes [2 à 15 de l'article 14] répond aux exigences de son cadre juridique de protection des données à caractère personnel* ***pour les transferts internationaux de données à caractère personnel****, et aucune autre autorisation de transfert n'est requise en vertu de ce cadre juridique. Une Partie ne peut refuser ou empêcher les transferts de données vers une autre Partie en vertu du présent Protocole que pour des raisons de protection des données: dans les conditions énoncées au paragraphe 15 [...]*»[52].

40. Cela signifie que si des États membres sont parties au protocole, ils reconnaissent que ledit protocole prévoit des garanties appropriées pour le transfert de données à caractère personnel. Il convient donc d'apprécier si des garanties appropriées sont prévues dans le protocole pour les transferts effectués par les autorités répressives ou des entités privées d'un État membre.

41. À cet égard, le CEPD comprend que l'article 14, paragraphe 1, point d), signifie qu'il est interdit aux États membres de refuser ou d'empêcher le transfert des données demandées pour des

raisons liées à l'application de leur propre **cadre juridique pour les transferts internationaux de données à caractère personnel**, même dans un cas particulier. En d'autres termes, des conditions spécifiques supplémentaires applicables aux transferts de données à caractère personnel ne peuvent pas être invoquées pour refuser ou empêcher un transfert vers une partie au protocole en tant que telle. Toutefois, si des garanties supplémentaires s'avéraient nécessaires dans un cas particulier, le protocole prévoit des moyens d'assurer des garanties supplémentaires au titre du chapitre II (Mesures de coopération renforcée) (voir section 4.4.). Enfin, il convient de souligner que seule une demande valable au titre du protocole, qui répond notamment aux exigences énoncées aux articles 13 et 14, peut entraîner l'obligation d'assister la partie requérante et, partant, de transférer des données.

4.2. Principe de proportionnalité

42. L'**article 13** du protocole exige, conformément à l'article 15 de la convention sur la cybercriminalité[53], qui fait expressément référence à l'application du principe de proportionnalité, que «*chaque Partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés*». Il s'applique à toutes les dispositions du protocole.

43. Le CEPD note également avec satisfaction que l'**article 14, paragraphe 2, point b)**, prévoit que, lors de la recherche et du traitement de données à caractère personnel[54], «*la Partie destinataire veille, dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement*»[55]. Bien que le protocole ne précise pas ce que signifie «pertinent et non excessif», le paragraphe 231 du rapport explicatif précise que cette exigence peut être mise en œuvre au moyen des «*principes de nécessité et de proportionnalité*».

44. En outre, l'**article 14, paragraphe 2, point a)**, précise que «*la Partie destinataire de données à caractère personnel traite lesdites données aux fins prévues à l'article 2*[56]*. Elle ne procède pas à d'autres traitements des données à caractère personnel dans un but incompatible avec cet article, et elle ne traite pas non plus les données lorsque son cadre juridique ne l'autorise pas*». Il découle en particulier de l'article 2 du protocole, comme expliqué plus en détail dans le rapport explicatif, que les dispositions du protocole ne peuvent pas être utilisées pour la production en masse ou en vrac de données[57].

45. En outre, comme indiqué ci-dessus, le chapitre II du protocole (Mesures de coopération renforcée) prévoit des voies supplémentaires de mise en œuvre du principe de proportionnalité.

46. Le CEPD est d'avis que l'application de ce principe[58] et la possibilité de refuser partiellement ou totalement de donner suite à une demande au titre du protocole fondée sur la proportionnalité découlent également de ce chapitre, qui prévoit la possibilité d'ajouter des conditions à la fourniture des informations demandées[59] ou des motifs de refus au titre des articles 7, 8 et 10, tels que l'article 27, paragraphe 4, de la convention sur la cybercriminalité[60].

4.3. Protection des données à caractère personnel

47. L'article 14, paragraphes 2 à 15, énonce les principes fondamentaux de la protection des données, qui couvrent toutes les formes de coopération prévues dans le protocole.

48. Ces principes couvrent ceux prévus par le RGPD et la directive (UE) 2016/680, à savoir: la limitation de la finalité, la minimisation des données, l'exactitude, la sécurité et l'intégrité, les données sensibles, les obligations applicables aux responsables du traitement (en ce qui

concerne la limitation de la conservation et du stockage, la prise de décision automatisée, les registres et journaux, ainsi qu'en ce qui concerne le partage ultérieur et les transferts ultérieurs), les droits individuels (en matière de transparence et de notification, d'accès, de rectification, y compris l'effacement) et les recours judiciaires et non judiciaires, ainsi que le contrôle indépendant et effectif par une ou plusieurs autorités (voir section 5).

4.3.1. Principes de limitation de la finalité et de minimisation des données

49. Comme indiqué ci-dessus, **des transferts de données à caractère personnel par une autorité répressive d'un État membre** vers un pays tiers peuvent avoir lieu si cela est nécessaire aux fins de la recherche, de la détection ou de la poursuite d'infractions pénales.

50. À cet égard, conformément à l'**article 2** du protocole, les mesures décrites dans le protocole s'appliquent «*à des enquêtes ou procédures pénales **spécifiques** concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique; et pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales **spécifiques** concernant les infractions pénales établies dans le Premier Protocole*»[61].

51. Cet objectif relève des finalités des transferts au titre de la directive (UE) 2016/680[62].

52. Le CEPD se félicite que, conformément à l'**article 14, paragraphe 2, point a), le traitement des données à caractère personnel reçues en vertu du protocole**[63] **soit limité au champ d'application de celui-ci**.

53. **En ce qui concerne le traitement ultérieur des données reçues**[64], le CEPD se félicite de **l'interdiction énoncée à l'article 14, paragraphe 2, de procéder au traitement ultérieur des données à caractère personnel à des fins incompatibles**[65] **et lorsque le droit interne de la partie ne le permet pas**. À cet égard, le CEPD se réjouit que le rapport explicatif encourage les autorités compétentes à procéder à une évaluation globale des circonstances spécifiques, telles que: «*(i) le rapport entre le but initial et le but supplémentaire ultérieur (établi par un éventuel lien objectif, par exemple); (ii) les conséquences (potentielles) pour les personnes concernées de l'utilisation supplémentaire envisagée, en tenant compte de la nature des données à caractère personnel (leur sensibilité, par exemple); (iii) les attentes raisonnables potentielles des personnes concernées quant au but de cette utilisation supplémentaire et à l'égard des entités qui pourraient traiter les données, et (iv) la manière dont les données seront traitées et protégées contre toute utilisation indue*»[66].

54. Comme indiqué ci-dessus, le traitement ultérieur des données à caractère personnel reçues en vertu du protocole à des fins compatibles n'est autorisé au titre du protocole que dans la mesure où il est conforme à l'article 13, tel qu'il a été mis en œuvre par chaque partie conformément aux principes pertinents de son droit interne[67].

55. Le CEPD note en outre que l'**article 14, paragraphe 2, point b)**, prévoit que la partie destinataire veille, dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement[68].

56. En outre, l'**article 14, paragraphe 2, point a)**, précise que «*[l]e présent article ne porte pas atteinte à la capacité de la Partie opérant le transfert*[69] *d'imposer des conditions supplémentaires en vertu du présent Protocole dans une situation spécifique; toutefois, ces conditions n'incluent pas des conditions génériques de protection des données*»[70], par exemple en exigeant que la partie requérante dispose d'une autorité spécialisée en matière de protection des données, alors que

des systèmes de contrôle différents sont acceptés en vertu de l'article 14[71]. Selon le rapport explicatif[72], ces conditions peuvent être imposées dans la mesure prévue au chapitre II du protocole.

57. Le CEPD croit donc comprendre que, si l'autorité destinataire n'était pas en mesure de respecter tout ou partie de ces conditions supplémentaires, le refus, la prévention ou la limitation, selon le cas, des données transférées pourrait, dans un cas spécifique, ne pas relever de cette dernière interdiction, étant donné qu'elle sera fondée sur les circonstances spécifiques de l'espèce.

58. S'agissant des **données transférées dans le cadre de la demande ou de l'injonction**, le chapitre II du protocole contient des dispositions spécifiques permettant à la partie requérante d'inclure dans sa demande ou dans son injonction toute instruction de procédure spéciale, y compris toute demande de confidentialité ou de non-divulgation des données à caractère personnel au déclarant, à l'abonné ou à d'autres tiers[73]. Il convient toutefois de noter que le protocole ne fait que créer un canal de coopération, mais n'impose pas l'obligation de demander une entraide sur ce fondement. Par conséquent, si la demande de garanties supplémentaires présentée par l'autorité requérante n'est pas satisfaite, le protocole laisse aux parties la possibilité d'utiliser d'autres canaux de coopération disponibles par ailleurs (article 5, paragraphe 7). Par conséquent, le CEPD comprend qu'en ce qui concerne les États membres, ces autres mécanismes de coopération pourraient être utilisés pour autant qu'ils soient conformes au droit de l'Union.

59. En ce qui concerne **les données demandées**, le CEPD note avec satisfaction que l'article 6 prévoit l'obligation d'utiliser les données demandées uniquement pour l'enquête ou la procédure pénale spécifique pour laquelle les données sont demandées. L'article 7, paragraphe 5, point c) ii) – qui, selon la proposition de la Commission, serait applicable dans les États membres –, et les articles 8 et 10 du protocole permettent à la partie requise de subordonner la fourniture des renseignements ou des pièces en réponse à une demande à la condition qu'elles ne soient pas utilisées pour des enquêtes ou des procédures autres que celles mentionnées dans la demande[74]. Conformément à l'article 9, paragraphe 6, du protocole, la partie requise peut spécifier les conditions dans lesquelles elle fournirait les données, ce qui pourrait donc inclure une limitation ou une autre condition quant à leur utilisation ultérieure, telle qu'être informée de ce traitement ultérieur. La possibilité d'imposer une limitation de l'utilisation des données reçues en vertu du protocole est confirmée par le rapport explicatif, qui clarifie davantage les exceptions à cette possibilité[75].

60. S'agissant des transferts au titre de l'article 7, le rapport explicatif[76] précise que la procédure visée au paragraphe 5, point d)[77], «*peut également fournir l'occasion de clarifier certains aspects de la confidentialité des informations recherchées ainsi que toute limitation d'utilisation envisagée par l'autorité sollicitant les données*».

61. Par conséquent, bien que le CEPD regrette qu'aucun mécanisme général n'ait été prévu dans le protocole pour informer les autorités compétentes des États membres concernés d'un traitement ultérieur, il note que le protocole offre un cadre qui permet à la partie transférant des données d'imposer une limitation quant à leur utilisation ultérieure et qui pourrait être utilisé par les parties pour être tenues informées d'un traitement ultérieur éventuel. À cet égard, le rapport explicatif précise que «*le matériel peut être utilisé à d'autres fins lorsque le consentement préalable d'une Partie transférante a été obtenu*»[78]. Une fois entré en vigueur, le protocole créerait un environnement favorable afin que les parties conviennent bilatéralement, le cas échéant, de toute autre mesure de transparence, telle que des codes de traitement.

4.3.2. Principes de limitation de la conservation et de conservation des données

62. L'article 14, paragraphe 5, du protocole prévoit l'obligation de ne conserver les données à caractère personnel que pendant la durée nécessaire et appropriée au regard des finalités spécifiques, conformément à l'article 2 du protocole, pour lesquelles les données sont traitées. Les données peuvent donc être conservées pendant la durée de l'enquête et de la procédure ultérieure et pour un traitement ultérieur qui n'est pas incompatible avec la finalité initiale. Afin de se conformer à cette obligation, les parties doivent prévoir dans leur cadre juridique interne des périodes de conservation déterminées et/ou revoir la nécessité de poursuivre la conservation à intervalles programmés. Selon le rapport explicatif, les parties «*devraient garantir dans leur cadre juridique que les autorités compétentes élaborent des règles et/ou procédures internes pour la mise en œuvre des durées de conservation déterminées et/ou des révisions périodiques de la nécessité de prolonger la conservation. Lorsque la durée de conservation est écoulée ou lorsque la Partie a établi, dans le cadre de la révision périodique, qu'il n'est plus nécessaire de conserver les données, celles-ci doivent être supprimées ou anonymisées*»[79].

4.3.3. Principe d'exactitude

63. L'article 14, paragraphe 3, du protocole dispose que chaque partie prend des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte et complète et soit aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi, compte tenu des buts dans lesquels elles sont traitées. Selon le rapport explicatif, «*[l]es Parties sont encouragées à prendre des mesures raisonnables pour s'assurer que, lorsque des données communiquées à une autre autorité ou reçues d'une autre autorité se révèlent inexactes ou obsolètes, cette autre autorité en est informée aussi rapidement que possible afin qu'il puisse être procédé aux corrections nécessaires et appropriées compte tenu des finalités du traitement*»[80].

4.3.4. Principes de sécurité, d'intégrité et de confidentialité

64. Le protocole soulève d'importantes questions concernant la sécurité des données à caractère personnel transférées. Le CEPD tient à souligner que garantir la sécurité des données à caractère personnel est non seulement une obligation claire imposée par le droit de l'Union[81], mais est aussi reconnu par la CJUE comme un caractère essentiel du droit fondamental à la protection des données. En outre, la sécurité des données est primordiale afin de garantir le secret des enquêtes et la confidentialité des procédures pénales.

65. Le CEPD se félicite donc de l'article 14, paragraphe 7, qui impose aux parties l'obligation de veiller à disposer de mesures techniques, physiques et organisationnelles appropriées pour la protection des données à caractère personnel et, en cas d'incident lié à la sécurité «*entraînant un risque significatif de préjudice matériel ou non matériel à des personnes ou l'autre Partie*», de prendre rapidement les mesures appropriées pour atténuer ce préjudice et prévoit que la partie destinataire notifie un incident de sécurité à l'autorité transférante et à la personne concernée.

66. Le CEPD prend également note avec satisfaction de l'explication donnée dans le rapport explicatif[82].

67. En outre, le chapitre II du protocole prévoit expressément que lorsqu'une demande ou une injonction est présentée sous forme électronique, un niveau approprié de sécurité et d'authentification peut être exigé[83].

4.3.5. Tenue des registres ou journaux (principe de responsabilité)

68. Le CEPD se félicite de l'obligation, prévue à l'article 14, paragraphe 8, de conserver des registres ou de disposer d'autres moyens appropriés, tels que l'enregistrement des activités[84], pour montrer comment les données à caractère personnel d'un individu sont consultées, utilisées et divulguées dans un cas particulier. Il regrette toutefois que cette obligation ne soit pas plus détaillée quant aux informations à fournir. Il note également avec désapprobation que cette obligation ne s'applique qu'à certaines activités de traitement (accès, utilisation et divulgation) et pas à d'autres, telles que le stockage.

4.3.6. Données sensibles

69. Conformément à la jurisprudence de la CJUE[85], la nécessité de disposer de garanties s'applique en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles.

70. S'agissant de **ce qui constitue une catégorie particulière de données à caractère personnel en vertu du protocole,** le CEPD note avec satisfaction que l'article 14, paragraphe 4, du protocole inclut les «données à caractère personnel révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale, ainsi que [...] de données génétiques, de données biométriques *considérées comme sensibles compte tenu des risques qu'elles comportent*; ou de données à caractère personnel concernant la santé ou la sexualité»[86]; Cette disposition n'autorise le traitement de telles données sensibles que «*moyennant des garanties appropriées pour se prémunir contre le risque d'effets préjudiciables injustifiés résultant de l'utilisation de ces données*, en particulier contre la discrimination illicite»[87].

71. Il convient de noter que l'article 14, paragraphe 2, point b) – qui doit être lu en combinaison avec l'article 13 (voir ci-dessus) –, exige expressément que «*les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement*»[88] et que des garanties appropriées soient mises en place en cas de prise de décision automatisée (article 14, paragraphe 6, voir ci-dessous).

72. S'agissant du **traitement des données sensibles** – qu'il s'agisse des données contenues dans la demande ou des données demandées, il convient de noter qu'en ce qui concerne le principe de sécurité consacré par le protocole (voir ci-dessus), le rapport explicatif encourage les parties à concevoir et à mettre en œuvre des mesures qui tiennent compte de la sensibilité des données[89]. En outre, en cas de partage ultérieur au sein d'une partie, les données sont traitées conformément à l'article 14 et tout transfert ultérieur doit être autorisé par l'autorité transférante (article 14, paragraphe 9 et 10, voir ci-dessous).

73. En ce qui concerne **le transfert de données en réponse à une demande ou à une injonction émise** en vertu du protocole, une autorité transférante peut, dans un cas particulier, ajouter des conditions relatives à l'utilisation des données [article 14, paragraphe 2, point a)] dans la mesure prévue au chapitre II du protocole (Mesures de coopération renforcée). Le chapitre II prévoit soit une demande non contraignante avec la possibilité de prévoir des conditions en vertu du droit national – qui pourraient donc être des conditions spécifiques liées à la catégorie particulière de données en cause – d'une part, ou, d'autre part, la possibilité de coopérer au titre des articles 7, 8 et 10, avec la possibilité soit d'ajouter des conditions spécifiques – qui pourraient donc être liées à la catégorie particulière de données en cause[90] –, soit de refuser de transférer les données demandées si, malgré les garanties imposées par le protocole à l'injonction[91], celle-ci devait constituer une violation des intérêts essentiels de la

partie requise (article 27, paragraphe 4, de la convention sur la cybercriminalité) ou être fondée sur l'article 25, paragraphe 4, de la convention sur la cybercriminalité[92].

74. S'agissant des **données transférées dans le cadre de la demande ou de l'injonction**, le chapitre II du protocole contient des dispositions spécifiques permettant à la partie requérante d'inclure dans sa demande ou dans son injonction toute instruction de procédure spéciale, y compris toute demande de confidentialité ou de non-divulgation des données à caractère personnel au déclarant, à l'abonné ou à d'autres tiers[93].

75. Le CEPD estime donc qu'il serait possible qu'une autorité exige, dans un cas spécifique, des garanties supplémentaires pour le traitement des données biométriques par la partie destinataire, même si les données biométriques ne sont pas considérées comme des données sensibles au sens du paragraphe 4 par la partie destinataire.

4.3.7. Décisions automatisées

76. Conformément à la jurisprudence de la CJUE, «*[l]a nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière des données à caractère personnel que sont les données sensibles*»[94].

77. Le CEPD se félicite du fait que l'article 14, paragraphe 6, interdise les décisions automatisées «*fondées uniquement sur un traitement automatisé des données à caractère personnel*» lorsqu'elles ont «un effet défavorable significatif sur les intérêts pertinents» de la personne concernée, sauf «*autorisation dans le droit interne et avec des garanties appropriées*». Ces garanties contre un effet défavorable significatif sur les intérêts pertinents de la personne concernée «*prévoient la possibilité d'obtenir une intervention humaine*». Cela garantit qu'aucune décision automatisée fondée sur les données reçues en vertu du protocole ne soit prise sans qu'il existe une possibilité d'intervention humaine et sans garanties appropriées. Cela est particulièrement important dans le domaine répressif, où les conséquences du profilage sur les individus sont potentiellement plus graves.

78. Il convient de relever que le rapport explicatif mentionne que «*[d]es garanties appropriées sont essentielles pour réduire l'impact potentiel sur les intérêts en jeu pour la personne à laquelle les données à caractère personnel se rapportent*»[95]. Cela doit être lu à la lumière de l'article 13, selon lequel les pouvoirs et procédures prévus par le protocole sont soumis aux conditions et garanties prévues par le droit interne de chaque partie, qui «*doit assurer une protection adéquate des droits de l'homme et des libertés*».

79. En outre, en ce qui concerne les **catégories particulières de données à caractère personnel** reçues et traitées par une autorité répressive en vertu du protocole, celui-ci prévoit que le traitement des données sensibles n'est effectué que moyennant des garanties appropriées pour se prémunir «*contre le risque d'effets préjudiciables injustifiés résultant de l'utilisation de ces données*»[96], en particulier contre la discrimination illicite (article 14, paragraphe 6, lu en combinaison avec l'article 14, paragraphe 4).

80. Enfin, comme indiqué dans la section ci-dessus relative à la limitation des finalités et à la minimisation des données, l'article 14, paragraphe 2, point b), du protocole impose à la partie requérante l'obligation de rechercher et de traiter des données qui soient pertinentes et qui ne soient pas excessives au regard de la finalité de ce traitement. En outre, le protocole permet à la partie transférante d'imposer des conditions quant à l'utilisation ultérieure des données [article 14, paragraphe 2, point a), à lire en combinaison avec le chapitre II – Mesures de coopération renforcée – voir ci-dessus]. Le CEPD comprend donc que, par exemple, l'autorité transférante d'un État membre peut, dans un cas particulier, imposer toute mesure spécifique de nature à sauvegarder les droits et libertés et les intérêts légitimes de la personne concernée dans le cas d'espèce. Il est donc

d'autant plus important que les États membres utilisent, comme le propose la Commission, la déclaration prévue à l'article 7, paragraphe 5, de sorte qu'une autorité intervienne toujours dans un État membre requis si le Conseil devait décider d'autoriser les États membres à signer et à ratifier, dans l'intérêt de l'Union, le protocole, sans se réserver le droit de ne pas appliquer l'article 7[97].

4.3.8. Partage ultérieur au sein d'une partie

81. Le CEPD se félicite des dispositions de l'article 14, paragraphe 9, relatives au partage ultérieur au sein d'une partie et note avec satisfaction que l'autre autorité dans la partie destinataire traite les données reçues en vertu du protocole conformément à l'article 14. Le rapport explicatif[98] précise que la procédure prévue à l'article 7, paragraphe 5, point d), qui, selon les propositions de la Commission, serait applicable dans les États membres (voir ci-dessous), peut également fournir l'occasion de clarifier certains aspects de la confidentialité des informations recherchées ainsi que toute limitation d'utilisation envisagée par l'autorité sollicitant les données. En outre, le chapitre II du protocole permet à l'autorité requérante de donner des instructions spéciales pour la non-divulgation de la demande aux abonnés ou à d'autres tiers[99].

4.3.9. Transfert ultérieur vers un autre État ou vers une organisation internationale

82. Le CEPD se félicite de la disposition de l'article 14, paragraphe 10, qui impose l'autorisation préalable de l'autorité de transfert pour le transfert par la partie destinataire vers un autre État ou vers une organisation internationale.

4.3.10. Consultation et suspension

83. Le CEPD se félicite que le protocole prévoie, en son article 14, paragraphe 15, une disposition spécifique permettant la suspension du transfert vers une partie au protocole si celle-ci «*viole de manière systématique ou flagrante les dispositions [de l'article 14] ou qu'une violation flagrante est imminente*».

84. En particulier, s'agissant du fait que l'article 14, paragraphe 1, point d), interdit toute nouvelle autorisation de transfert, le CEPD rappelle que l'établissement, dans les États membres, d'autorités de contrôle nationales indépendantes est un élément essentiel de la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel[100]. Les autorités nationales de contrôle sont chargées de contrôler le respect du droit de l'Union en matière de protection des données, conformément à l'article 8, paragraphe 3, de la Charte, et chaque autorité est investie du pouvoir de vérifier si un transfert de données à caractère personnel de son propre État membre vers un pays tiers est conforme à la législation en matière de protection des données, même si le système juridique d'un pays tiers a été jugé adéquat ou si une présomption de conformité est introduite sur la base d'un accord.

4.3.11. Révision

85. Le CEPD se félicite de l'introduction, en vertu de l'article 23, d'un mécanisme permettant d'évaluer périodiquement l'utilisation et la mise en œuvre effectives des dispositions du protocole et de la clarification, dans le rapport explicatif[101], selon laquelle «*[c]ompte tenu de l'expertise nécessaire à l'évaluation de l'utilisation et de la mise en œuvre de certaines dispositions du présent Protocole, notamment de l'article 14 sur la protection des données, les Parties peuvent envisager d'associer leurs experts en la matière aux évaluations*».

4.4. Mesures de coopération renforcée

4.4.1. Observations générales

86. Le CEPD tient tout d'abord à rappeler que, conformément au considérant 71 de la directive (UE) 2016/680, lorsque les transferts effectués par les autorités compétentes en matière répressive ne sont pas fondés sur une décision d'adéquation, le responsable du traitement devrait tenir compte du fait que les données à caractère personnel ne seront pas utilisées pour demander, prononcer ou exécuter une condamnation à la **peine de mort** ou toute forme de traitement cruel et inhumain. Il se félicite dès lors que les dispositions du protocole relatives à la coopération au titre des articles 7, 8 et 10, en introduisant l'article 27, paragraphe 4, de la convention sur la cybercriminalité comme motif de refus de transfert, permettent à une partie transférante de tenir compte de ce risque et de refuser de transférer des données sur cette base.

87. En outre, le CEPD comprend que les **privilèges et immunités** peuvent être invoqués par une partie requise comme motif de refus d'émettre des injonctions de produire au cas par cas, sur la base de l'article 25, paragraphe 4, et de l'article 27, paragraphe 4, de la convention sur la cybercriminalité[102] ou peuvent être ajoutés par une partie dans le cadre des conditions raisonnables prévues par le droit interne pour les demandes non contraignantes au titre des articles 6 et 9[103].

88. Enfin, le CEPD se félicite qu'aucune disposition relative à l'**accès direct des autorités répressives aux données** n'ait été incluse dans le texte final du protocole.

4.4.2. Divulgation directe de données relatives aux abonnés par les fournisseurs de services aux autorités compétentes d'une autre partie (article 7)

4.4.2.1. Limitation du statut des autorités requérantes par la partie requise

89. Le CEPD se félicite que l'annexe donne instruction aux États membres de faire la déclaration prévue à l'article 7, paragraphe 2, point b), indiquant que les injonctions adressées aux fournisseurs de services établis sur leur territoire doivent être émises par un procureur ou une autre autorité judiciaire ou sous la supervision de cette autorité, ou sous une autre forme de supervision indépendante.

4.4.2.2. Intervention systématique d'une autorité judiciaire dans la partie requise

90. Le CEPD se félicite de l'instruction donnée aux États membres dans l'annexe de notifier, conformément à l'article 7, paragraphe 5, point a), du protocole, que, lorsqu'une injonction est adressée en vertu de l'article 7, paragraphe 1, à un fournisseur de services établi sur leur territoire, la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure à leurs autorités est requise. Ces autorités ont le pouvoir d'ordonner au fournisseur de services de ne pas divulguer les informations relatives à l'abonné si:

    i. cette divulgation risque de porter préjudice à des enquêtes ou procédures pénales menées sur le territoire de cette partie; ou

    ii. les conditions ou les motifs de refus visés à l'article 25, paragraphe 4, et à l'article 27, paragraphe 4, de la convention sur la cybercriminalité[104] s'appliquent parce que les données relatives à l'abonné avaient fait l'objet d'une demande d'entraide judiciaire.

91. À cet égard, conformément à l'article 7, paragraphe 5, point e), les parties désignent une autorité unique pour recevoir cette notification. Toutefois, ni l'article ni l'annexe ne mentionnent spécifiquement le type d'autorité. Étant donné que l'autorité compétente ordonnant la divulgation des informations pourrait ne pas être une autorité judiciaire ou une autre autorité indépendante[105], le CEPD **recommande d'inviter les États membres à désigner une autorité judiciaire ou une autre autorité indépendante chargée de recevoir la notification** afin de donner à ces autorités la possibilité de contrôler efficacement la conformité des injonctions avec la convention sur la cybercriminalité et d'exécuter les actions décrites au paragraphe 5, points b), c) et d). Une telle participation serait également plus conforme à l'article 82, paragraphe 1, TFUE.

92. À cet égard, le CEPD rappelle que, dans sa jurisprudence relative à l'accès aux données de communications à des fins répressives, **la CJUE a subordonné la possibilité de prévoir un tel accès, entre autres critères, et «*sauf cas d'urgence dûment justifiés*»[106], à un «*contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante*»**, «*à la suite d'une demande motivée de[s] autorités [nationales compétentes] présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales*»[107]. L'implication systématique des autorités judiciaires des parties requises est également essentielle pour préserver l'application du principe de la double incrimination[108] dans le domaine de la coopération judiciaire, car elle permettrait à une autorité adéquate et appropriée de vérifier les circonstances conduisant à l'application de ce principe. Le CEPD rappelle que le principe de la double incrimination vise à apporter une garantie supplémentaire afin de s'assurer qu'un État ne puisse pas invoquer l'aide d'un autre État pour appliquer une sanction pénale qui n'existe pas dans le droit d'un autre État.

4.4.2.3. Définitions et types de données

93. Le CEPD note que la définition des données relatives aux abonnés, au sens de l'article 18, paragraphe 3, de la convention sur la cybercriminalité, peut également inclure les informations qui, en vertu du droit de l'Union, constituent des données relatives au trafic. En effet, les informations nécessaires à l'identification d'un abonné à un service peuvent effectivement comprendre certaines informations relatives à l'adresse IP (Protocole Internet) – par exemple, l'adresse IP utilisée au moment de la création d'un compte, l'adresse IP de connexion la plus récente ou les adresses IP de connexion utilisées à un moment donné, qui, en vertu du droit de l'Union, constituent des données relatives au trafic concernant la transmission d'une communication[109].

94. En outre, conformément à la jurisprudence pertinente de la CJUE, pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il n'est pas pertinent de savoir si les informations relatives à la vie privée concernée sont sensibles ou si les personnes concernées ont été gênées de quelque manière que ce soit. La CJUE a en outre jugé dans son arrêt dans les affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB, que des métadonnées telles que les données relatives au trafic permettent d'établir un profil des personnes concernées, des informations qui ne sont pas moins sensibles, eu égard au droit au respect de la vie privée, que le contenu réel des communications[110].

95. Étant donné que l'équilibre entre les types d'infractions pour lesquelles une injonction peut être émise et les catégories de données concernées devrait être apprécié afin de limiter la possibilité de présenter une injonction de produire des données qui pourraient être considérées comme des données relatives au trafic dont l'accès est uniquement justifié par la lutte contre la criminalité grave, **le CEPD recommande aux États membres de se réserver le droit de ne pas appliquer l'article 7 pour certains types de numéros d'accès, conformément à l'article 7, paragraphe 9, point b), contrairement aux instructions de la Commission**

figurant en annexe, afin d'assurer une participation plus importante des autorités de l'État requis. Il note à cet égard que le protocole prévoit une autre voie pour la production accélérée de données au titre de l'article 8 entre les autorités compétentes des parties concernées.

4.4.3. Donner effet aux injonctions d'une autre partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic (article 8)

96. Le CEPD se félicite de l'instruction donnée par la Commission aux États membres de déclarer, en vertu de l'article 8, paragraphe 4, que des informations supplémentaires sont nécessaires pour donner effet à des injonctions émises au titre de l'article 8, paragraphe 1, qui dépendront des circonstances de l'injonction et de l'enquête ou de la procédure y afférente; ceci étant particulièrement important pour permettre aux autorités de prendre une décision adéquate conformément à l'article 8, paragraphe 8, du protocole.

97. Le CEPD note en outre que la Commission charge «*les États membres qui participent à la coopération renforcée établie par le règlement (UE) 2017/1939 mettant en œuvre une coopération renforcée concernant la création du Parquet européen [d'inclure] le Parquet européen, lorsque ce dernier exerce ses compétences prévues aux articles 22, 23 et 25 du règlement (UE) 2017/1939, parmi les autorités dont les coordonnées auront été communiquées en application de l'article 8, paragraphe 10, points a) et b)*», c'est-à-dire parmi les autorités désignées pour soumettre ou recevoir une injonction de production accélérée de données relatives aux informations sur les abonnés et au trafic.

98. Le CEPD rappelle que, selon la jurisprudence de la CJUE, celle-ci a limité la possibilité de prévoir un tel accès, entre autres critères, et «sauf cas d'urgence dûment justifiés»[111] à un «contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante» (voir point 92 ci-dessus). Par conséquent, il souligne qu'un procureur d'un État membre et, par conséquent, le Parquet européen ne devraient pouvoir présenter une injonction ou transférer des données sur la base d'une injonction d'une autre partie en application de cette disposition que lorsqu'un contrôle est assuré par une autorité judiciaire ou par une entité indépendante au sens de la jurisprudence de la CJUE[112].

5. Droits opposables des personnes concernées et voies de recours effectives pour les personnes concernées

5.1. Droit à l'information, droit d'accès, droit de rectification et d'effacement

99. Le CEPD rappelle que les droits d'accès et de rectification sont des éléments essentiels du droit à la protection des données prévu à l'article 8, paragraphe 2, de la Charte. 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 une autorité lorsque l'exercice de ces droits est refusé pour protéger des informations sensibles en matière répressive.

100. Le protocole comprend des dispositions relatives au droit à être informé (article 14, paragraphe 11), au droit d'accès [article 14, paragraphe 12, point a) ii)] et au droit de rectification - qui comprend également le droit d'effacement et le droit de verrouillage

[article 14, paragraphe 12, point a) ii)] et le droit de ne pas faire l'objet de décisions automatisées (article 14, paragraphe 6, voir plus haut).

101. 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[113]. Les personnes concernées n'ont généralement pas connaissance du fait que leurs données sont traitées (ou transférées) à des fins répressives. Le CEPD rappelle qu'en ce qui concerne les transferts effectués par des entités privées, la CJUE a jugé dans son avis 1/15 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*»[114].

102. Le CEPD se félicite donc de l'inclusion, en application de l'article 14, paragraphe 11, de l'obligation faite à chaque partie de notifier le traitement, par la publication de notifications générales ou d'une notification personnelle à la personne concernée. Si l'on peut déplorer que cette obligation ne comporte pas l'obligation de fournir les coordonnées du responsable du traitement, le CEPD note que le protocole impose l'obligation de notifier la base juridique et la ou les finalités du traitement, toute période de conservation ou de révision, le cas échéant, l'accès, la rectification et les recours possibles ainsi que les destinataires ou catégories de destinataires auxquels ces données sont communiquées.

103. Le droit à l'information s'applique également en cas de partage ultérieur, en ce qui concerne le traitement ultérieur des données par une autorité (article 14, paragraphe 9).

104. Le protocole garantit en outre la notification personnelle de la personne concernée lorsque le droit de la partie transférante le prévoit. Si l'autre partie a demandé que la communication des données reste confidentielle lorsque les conditions de limitation prévues par le protocole s'appliquent, cette notification personnelle n'a lieu qu'une fois que les limitations ne s'appliquent plus[115]. La notification personnelle peut être limitée dans les mêmes conditions que le droit d'accès (voir ci-dessous).

105. 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. En outre, s'agissant de l'article 7 de la Charte, la Cour a jugé que «*le droit fondamental au respect de la vie privée, consacré à cet article, implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite. Afin de pouvoir effectuer les vérifications nécessaires, cette personne doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement*»[116].

106. Le CEPD se félicite donc de l'inclusion, à l'article 14, paragraphe 12, **d'un droit d'accès et de rectification, qui inclut le droit à l'effacement**.

107. Le protocole prévoit que le droit d'accès peut faire l'objet de restrictions [point a)]. 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. À cet égard, le CEPD accueille favorablement le fait que le protocole prévoie expressément que les limitations doivent être proportionnées et nécessaires pour protéger les droits et libertés d'autrui ou des objectifs importants d'intérêt public général et tenir dûment compte des intérêts légitimes des personnes concernées. Il regrette toutefois que le protocole n'impose pas au cadre juridique

interne des parties de veiller à ce que les personnes concernées puissent, de facto, avoir accès à leurs propres données, même si cette possibilité est limitée ou exercée par une autorité.

108. Le CEPD regrette que le protocole autorise l'imposition de frais d'accès [point b)]. Il note toutefois qu'ils doivent rester dans les limites du raisonnable et ne pas être excessifs «au vu des ressources impliquées» «afin de ne pas dissuader ou décourager les intéressés», selon les termes du rapport explicatif[117]. Le CEPD croit également comprendre que ces frais ne peuvent pas être imposés à l'exercice du droit de rectification, y compris le droit à l'effacement.

5.2. Recours juridictionnel et administratifs

109. Le CEPD rappelle que, dans le contexte différent d'une décision d'adéquation (la «sphère de sécurité»), la CJUE a conclu[118] que 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*»[119].

110. En outre, la CJUE a souligné qu'il était essentiel que les personnes puissent introduire des plaintes auprès d'autorités de contrôle indépendantes[120] et, partant, demander à exercer un recours administratif.

111. Le CEPD se félicite dès lors que l'article 14, paragraphe 13, prévoie que chaque partie dispose de voies de recours judiciaires et non judiciaires effectives pour permettre un recours en cas de violation de cet article.

5.3. Supervision: contrôle par une autorité indépendante

112. L'article 16 TFUE et l'article 8, paragraphe 3, de la Charte contiennent 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 superviser les activités de traitement de données, y compris le transfert de données vers des pays tiers, il est en outre nécessaire de garantir un contrôle indépendant efficace une fois que les données ont été transférées dans les pays tiers destinataires.

113. Le CEPD rappelle que, conformément à la jurisprudence de la CJUE[121], 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 supervise, 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*»[122].

114. Le CEPD se félicite de l'article 14, paragraphe 14, relatif au contrôle, qui exige de chaque partie qu'elle dispose d'une autorité de contrôle indépendante et précise les pouvoirs effectifs que cette ou ces autorités peuvent exercer à l'égard des autorités auxquelles des données à caractère personnel seraient transférées sur la base du protocole. Il ressort du rapport explicatif

que *[l]es autorités devraient remplir leur mission et exercer leurs compétences de manière impartiale. Elles devraient pouvoir agir en étant dégagées de toute influence extérieure susceptible d'interférer dans l'exercice indépendant de leurs fonctions et compétences. Elles ne devraient, en particulier, recevoir aucune instruction, dans une affaire donnée, portant sur l'exercice de leurs compétences en matière d'enquête et/ou sur la prise de mesures correctives. Enfin, il est important qu'elles disposent des compétences, des connaissances et de l'expertise nécessaires pour mener à bien leurs tâches et qu'elles soient dotées des ressources financières, techniques et humaines appropriées pour pouvoir exercer effectivement leurs fonctions*»[123]. Le CEPD souligne que, s'il devait être établi dans la pratique qu'une autre partie ne prévoit pas d'autorité de supervision indépendante substantiellement équivalente aux normes de l'UE, les États membres devraient être autorisés à se prévaloir de la disposition relative à la suspension en cas de violation systématique ou substantielle de cet article 14, en application du paragraphe 15 dudit article.

115. Bien qu'aucun mécanisme de coopération spécifique entre les autorités de surveillance respectives ne soit prévu par le protocole et que les parties ne soient pas tenues de notifier leur autorité de supervision, le CEPD note avec satisfaction que, dans le rapport explicatif, les parties sont encouragées à promouvoir la coopération entre leurs autorités de supervision respectives. «*Des consultations entre les autorités respectives des Parties dans l'exercice de leurs fonctions de surveillance en vertu du présent article peuvent avoir lieu, le cas échéant. Cela peut inclure l'échange d'informations et de meilleures pratiques*»[124].

6. Rapport entre la disposition relative à la protection des données (article 14) du protocole et d'autres accords

116. Compte tenu du caractère multilatéral du protocole, son article 14, paragraphe 1, points b) et c), permet aux parties, dans leurs relations bilatérales, de convenir, sous certaines conditions, d'autres moyens d'assurer la protection des données à caractère personnel transférées en vertu du protocole.

6.1. Relations entre l'Union européenne et les États-Unis d'Amérique

117. Alors que les garanties prévues à l'article 14, paragraphes 2 à 15, s'appliquent par défaut aux parties qui reçoivent des données à caractère personnel, sur la base de l'article 14, paragraphe 1, point b), «*[s] i, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie transférante et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application de cet accord, aux données à caractère personnel reçues en vertu de ce Protocole en lieu et place des paragraphes 2 à 15, sauf accord contraire entre les Parties concernées*».

118. Le CEPD note que, selon le rapport explicatif[125], un exemple d'un tel accord est l'accord-cadre entre les États-Unis d'Amérique et l'Union européenne[126] et que «*les termes de ces accords s'appliquent en lieu et place des paragraphes 2 à 15 en ce qui concerne les mesures entrant dans leur champ d'application*».

119. À cet égard, le CEPD se félicite que la Commission propose aux États membres de communiquer aux autorités des États-Unis d'Amérique l'interprétation de l'UE sur ce point.

120. Le CEPD comprend qu'il est confirmé que l'accord-cadre UE-États-Unis s'appliquerait aux transferts de l'UE vers les États-Unis d'Amérique dans le cadre des dispositions énoncées dans le protocole concernant la **coopération entre les autorités.** Le CEPD déplore ce résultat.

121. En ce qui concerne l**es dispositions du protocole relatives à la coopération directe** (articles 6 et 7), le CEPD tient à rappeler que l'accord-cadre ne serait pas applicable[127]. Pour qu'il le soit, il devrait être modifié par un accord entre l'Union européenne et les États-Unis, qui devra contenir des garanties supplémentaires. Le CEPD renvoie à cet égard à son avis sur la recommandation de la Commission relative à une 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[128]. Par conséquent, le CEPD estime que, jusqu'à l'adoption et l'entrée en vigueur d'un tel accord entre les deux parties, les garanties prévues à l'article 14 du protocole s'appliqueraient au traitement des données à caractère personnel reçues par une partie en vertu des dispositions du protocole relatives à la coopération directe.

122. Le CEPD comprend que la communication proposée par la Commission vise à préciser que, pour la coopération directe prévue par le protocole, l'accord-cadre ne s'appliquerait pas entre l'UE et les États-Unis en lieu et place des paragraphes 2 à 15 de l'article 14 du protocole. Il découle en effet de l'article 14, paragraphe 1, point b), du protocole, lu en combinaison avec les exigences énoncées dans le droit de l'Union, que seul un instrument juridiquement contraignant conclu entre l'UE et les États-Unis sous la forme d'un accord international modifiant l'accord-cadre et prévoyant les garanties supplémentaires nécessaires pourrait remplir les conditions énoncées à l'article 14, paragraphe 1, point b), du protocole pour que ses dispositions relatives à la protection des données s'appliquent en lieu et place des paragraphes 2 à 15 de l'article 14 du protocole. Le CEPD **recommanderait donc, dans l'hypothèse où le Conseil déciderait d'autoriser les États membres à signer et à ratifier le protocole, de clarifier encore davantage la communication proposée, qui fait actuellement référence à un «accord spécifique de transfert»**.

6.2. Relations entre l'UE et d'autres pays tiers parties au protocole

123. L'article 14, paragraphe 1, point c), du protocole dispose que «*[s]i la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord décrit au paragraphe 1.b, elles peuvent déterminer d'un commun accord que le transfert de données à caractère personnel en vertu du présent Protocole peut avoir lieu sur la base d'autres accords ou arrangements entre les Parties concernées en lieu et place des paragraphes 2 à 15*»[129].

124. Le CEPD **se félicite de l'intention de la Commission**, dans son examen, de préciser que les États membres sont liés par le cadre juridique de l'UE, tel qu'il découle du chapitre V du RGPD et de la directive (UE) 2016/680, lorsqu'ils déterminent s'ils pourraient se prévaloir des dispositions de l'article 14, paragraphe 1, point c), du protocole pour appliquer d'autres dispositions en matière de protection des données convenues entre les parties sur les transferts de données à caractère personnel en vertu du protocole, en lieu et place des paragraphes 2 à 15 de l'article 14 dudit protocole.

125. Le CEPD **recommanderait toutefois de clarifier davantage cet examen dans l'hypothèse où le Conseil déciderait d'autoriser les États membres à signer et à ratifier le protocole**.

126. En particulier, il tient à souligner que lesdits accords devraient remplir les conditions énoncées au chapitre V du RGPD **et** dans la directive (UE) 2016/680.

127. Cet examen fait notamment référence à un «*accord ou arrangement [qui] prévoit lui-même des garanties appropriées en matière de protection des données conformément à l'article 46 du règlement général sur la protection des données*».

128. Le CEPD tient à souligner en outre qu'un objectif important du protocole consiste à fournir des garanties appropriées en matière de protection des données dans un accord international juridiquement contraignant aux fournisseurs de services de l'UE lorsqu'ils transfèrent des données à la demande des autorités de pays tiers. Étant donné que le protocole fait référence à des «accords ou arrangements entre les Parties concernées», le CEPD invite donc la Commission à expliquer quels accords ou arrangements peuvent prévoir des garanties appropriées en matière de protection des données conformément à l'article 46 du RGPD pour les transferts effectués par des fournisseurs de services ou des entités fournissant des services d'enregistrement de noms de domaine situés dans l'UE vers des autorités d'un pays tiers partie au protocole.

7. Conclusions

129. Compte tenu de la prolifération de la cybercriminalité et de l'importance croissante des preuves électroniques dans les enquêtes pénales et au vu de la complexité de l'obtention de ces preuves lorsqu'elles ne relèvent pas de la compétence des États membres, le CEPD comprend la nécessité pour les autorités répressives d'obtenir rapidement et efficacement des preuves électroniques afin de pouvoir lutter efficacement contre la criminalité.

130. Le CEPD est donc favorable à une réponse internationale assortie de garanties appropriées aux questions existantes dans ce contexte.

131. Le protocole vise à la fois à améliorer les canaux de coopération traditionnels et à établir une coopération directe entre les autorités répressives et les fournisseurs de services transfrontières. Il ne contient pas de dispositions sur l'accès direct aux données par les autorités répressives, ce dont le CEPD se réjouit.

132. Tout en reconnaissant qu'il n'est pas possible de reproduire entièrement la terminologie et les définitions du droit de l'UE dans un accord international multilatéral, le CEPD souligne que les garanties appropriées en matière de protection des données pour les personnes physiques doivent être prévues afin de respecter pleinement le droit de l'Union.

133. Le CEPD se félicite du fait que le protocole contienne un article spécifique sur la protection des données à caractère personnel. Il note également avec satisfaction les nombreuses garanties qui ont été incluses dans le protocole.

134. Le CEPD comprend qu'il est confirmé que l'accord-cadre UE-États-Unis s'appliquerait aux transferts de l'UE vers les États-Unis d'Amérique dans le cadre des dispositions énoncées dans le protocole concernant la coopération entre les autorités. Le CEPD déplore ce résultat.

135. En cas d'adoption d'une décision du Conseil autorisant les États membres à, respectivement, signer et ratifier, dans l'intérêt de l'Union, le protocole, le CEPD se félicite des propositions de la Commission visant à ce que les États membres fassent, dans l'intérêt de l'Union, la déclaration, la notification et la communication au titre de l'article 7, paragraphe 2, point b),

et de l'article 7, paragraphe 5, points a) et e), du protocole. Ces propositions garantissent que les fournisseurs de services de l'Union ne puissent être sollicités pour le transfert de données à caractère personnel que sur la base d'injonctions émises, dans le pays tiers requérant partie au Protocole, par un procureur ou une autre autorité judiciaire, ou sous la supervision d'un procureur ou d'une autre autorité judiciaire, ou sous une autre forme de supervision indépendante et sous le contrôle d'une autorité compétente dans l'État membre requis.

136. Le CEPD note également avec satisfaction la proposition selon laquelle les États membres font la déclaration visée à l'article 8, paragraphe 4, du protocole (sur la coopération entre les autorités compétentes pour donner suite aux injonctions de fournir les données relatives aux abonnés et au trafic), de sorte que des informations complémentaires soient nécessaires pour donner effet aux injonctions au titre de cette disposition.

137. Le CEPD formule les recommandations suivantes en ce qui concerne les futures décisions du Conseil, si le protocole devait être signé et ratifié par les États membres, dans l'intérêt de l'Union:

- certaines données relevant de la catégorie des données relatives aux abonnés au sens de la convention sur la cybercriminalité peuvent être considérées, en vertu du droit de l'Union, comme des données relatives au trafic impliquant une ingérence grave dans les droits fondamentaux de la personne concernée, dont l'accès ne peut être justifié que par la lutte contre la criminalité grave. Par conséquent, contrairement à la proposition de la Commission, le CEPD recommande aux États membres de se réserver le droit de ne pas appliquer l'article 7 du protocole sur la divulgation des données relatives aux abonnés par les fournisseurs de services directement aux autorités compétentes d'un autre pays en ce qui concerne certains types de numéros d'accès, conformément à l'article 7, paragraphe 9, point b);

- les États membres devraient désigner, conformément à l'article 7, paragraphe 5, point e), du protocole, une autorité judiciaire ou une autre autorité indépendante;

- la communication proposée par les États membres aux autorités des États-Unis, au moment de la signature ou du dépôt de leur instrument de ratification, d'acceptation ou d'approbation, en rapport avec l'accord-cadre UE-États-Unis, devrait être clarifiée;

- il y a lieu de modifier l'examen proposé à l'aune d'autres accords ou arrangements au titre de l'article 14, paragraphe 1, point c), du protocole, qui pourraient remplacer sa disposition relative à la protection des données (article 14).

138. Enfin, le CEPD souligne qu'un procureur d'un État membre et, partant, le Parquet européen ne devraient pouvoir émettre une injonction de produire ou de transférer des données sur la base de l'injonction d'une autre partie au titre de l'article 8 que s'il est établi que cette injonction fait l'objet d'un contrôle par une autorité judiciaire ou une entité indépendante au sens de la jurisprudence de la CJUE.

139. Le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir d'autres conseils au cours la procédure. Le présent avis est délivré sans préjudice des observations supplémentaires que le CEPD pourrait formuler sur la base d'informations disponibles ultérieurement.

Bruxelles, le 20 janvier 2022

[signature électronique]

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690
[5] 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 (STCE nº 185), COM(2019) 71 final.
[6] https://rm.coe.int/1680a49dab (version provisoire approuvée par le Comité des Ministres).
[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
[8] Avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un deuxième Protocole additionnel à la convention de Budapest sur la cybercriminalité du 2 avril 2019.
[9] Décision du Conseil adoptée le 6 juin 2019 autorisant la Commission européenne à participer, au nom de l'Union européenne, aux négociations relatives à un deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (STCE nº 185).
[10] «Contribution du comité européen de la protection des données à la consultation sur un projet de deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest) du 13 novembre 2019»; «Déclaration 02/2021 sur les nouveaux projets de dispositions du deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest), adoptée le 2 février 2021»; «Contribution de l'EDPB au 6e cycle de consultations sur le projet de deuxième Protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité du 4 mai 2021».
[11] Résolution du Parlement européen du 10 juin 2021 sur la stratégie de cybersécurité de l'Union européenne pour la décennie numérique.
[12] Article 21 du protocole.
[13] Considérant 10 des deux propositions de décisions du Conseil autorisant les États membres à signer et à ratifier, dans l'intérêt de l'Union européenne, le deuxième Protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques
[14] Proposition de décision du Conseil autorisant les États membres à signer, dans l'intérêt de l'Union européenne, le deuxième Protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques [COM(2021)718 final].
Proposition de décision du Conseil autorisant les États membres à signer, dans l'intérêt de l'Union européenne, le deuxième Protocole additionnel à la convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques [COM(2021)719 final].
Conformément aux considérants 14 et 15 de la proposition relative à la signature et aux considérants 13 et 14 de la proposition relative à la ratification, l'Irlande a la possibilité de participer à l'adoption et à l'application de la décision et le Danemark ne participe pas à l'adoption de la présente décision et n'est ni lié par celle-ci ni soumis à son application.
[15] Considérant 3 des propositions.
[16] Article 16, paragraphe 1. [...] [les Parties à la Convention, qui] peuvent exprimer leur consentement à être liées par:
a. la signature sans réserve de ratification, d'acceptation ou d'approbation; ou
b. la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.
2. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.
[17] Tous à l'exception de l'Irlande, qui a signé mais pas ratifié la convention, et s'est néanmoins engagée à poursuivre son adhésion.
[18] Voir l'état des signatures et ratifications concernant 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/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ZZawh58m
[19] Voir articles 23-35 de la convention sur la cybercriminalité.
[20] https://rm.coe.int/1680a49c9d Comme indiqué par le Comité des Ministres le 17 novembre 2021.
[21] Voir paragraphe 2 du rapport explicatif joint au protocole.
[22] Au sens de l'article 18, paragraphe 3, de la convention sur la cybercriminalité, l'expression «données relatives aux abonnés» désigne «toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant 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 services;
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 services».
[23] Au sens de la Convention de Budapest, l'expression «données relatives au trafic» désigne «toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent».
[24] Au sens de la convention sur la cybercriminalité, l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.
[25] Paragraphe 172 du rapport explicatif: «Étant donné que l'article 10 de ce Protocole est limité aux urgences justifiant une telle célérité, il est distinct de l'article 25, paragraphe 3, de la Convention, qui prévoit que les demandes d'entraide peuvent être transmises par des moyens de communication rapides en situations d'urgence qui ne sont pas d'un niveau d'urgence défini. En d'autres termes, l'article 25, paragraphe 3, a une portée plus large que l'article 10 du Protocole, puisqu'il couvre des situations non couvertes par ce dernier, par exemple les risques existants mais non imminents pour la vie ou la sécurité de personnes physiques, la destruction potentielle de preuves qui pourrait résulter d'un retard, le fait que la date d'un procès se rapproche ou autres types d'urgences. Alors que le mécanisme visé à l'article 25, paragraphe 3, prévoit une méthode plus rapide pour transmettre une demande et y répondre, les obligations en cas d'urgence relevant de l'article 10 du Protocole sont nettement plus lourdes; en d'autres termes, lorsqu'il existe un risque significatif et imminent pour la vie ou la sécurité d'une personne physique, le processus devrait être encore plus rapide (voir paragraphe 42 du présent rapport explicatif pour des exemples de situations d'urgence)».
[26] Paragraphes 77 et 169 du rapport explicatif.
[27] «Une Partie qui se réserve ce droit n'est pas autorisée à adresser des injonctions en vertu du paragraphe 1 à des fournisseurs de services sur le territoire d'autres Parties», rapport explicatif, paragraphes 122 et 123.
[28]«Une Partie qui émet des réserves concernant cet article n'est pas autorisée à soumettre des injonctions de production de données relatives au trafic à d'autres Parties en vertu du paragraphe 1», rapport explicatif, paragraphe 147.
[29] Annexe, section 1.
[30] Annexe, sections 2 et 3.
[31] «Réponse conjointe de l'EDPB et du CEPD à la commission LIBE concernant l'incidence du Cloud Act américain sur le cadre juridique européen en matière de protection des données à caractère personnel» (10 juillet 2019), https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[32] Affaire 181/73, R. & V. Haegemann/État belge, ECLI:EU:C:1974:41, point 5.
[33] Affaire C-308/06, Intertanko e.a., ECLI:EU:C:2008:312, point 42.
[34] Affaires jointes C-402/05 P et C-415/05 P, Kadi/Conseil, ECLI:EU:C:2008:461, point 285.
[35] Soit dans le cadre des demandes et injonctions des États membres, soit en réponse à ces demandes et injonctions.
[36] En réponse à une demande ou à une injonction au titre des articles 6 et 7 du protocole.
[37] Le paragraphe 99 du rapport explicatif précise qu'à «l'article 7, l'expression "fournisseur de services sur le territoire d'une autre Partie" nécessite que le fournisseur de services soit physiquement présent sur le territoire de l'autre Partie. En vertu de cet article, le simple fait, par exemple, qu'un fournisseur de services ait établi une relation contractuelle avec une entreprise dans un État partie, mais que le fournisseur de services lui-même ne soit pas physiquement présent sur le territoire de cette Partie, ne permettrait pas de considérer que le fournisseur de services se trouve "sur le territoire" de cette Partie. Le paragraphe 1 exige, en outre, que les données soient en la possession ou sous le contrôle du fournisseur de services». Voir également le paragraphe 77 du rapport explicatif en ce qui concerne l'article 6.
[38] 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).
[39] 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 (JO L 119 du 4.5.2016, p. 1).
[40] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592.
[41] Ibid., point 214.
[42] Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650, point 95.
[43] Voir paragraphe 76 du rapport explicatif: L'objectif de l'article 6 est de donner un cadre effectif et efficient d'obtention d'informations pour identifier ou contacter la personne ayant enregistré un nom de domaine. Les modalités de sa mise en œuvre dépendent des considérations légales et politiques des différentes Parties. Cet article entend compléter les politiques et pratiques actuelles et futures de gouvernance de l'internet».
[44] Paragraphe 100.

[45] Voir, par exemple, en l'absence d'accord international, la réponse conjointe de l'EDPB et du CEPD à la commission LIBE concernant l'incidence du Cloud Act américain sur le cadre juridique européen en matière de protection des données à caractère personnel, 10 juillet 2019.
[46] Article 6, paragraphe 2, du protocole et paragraphe 82 du rapport explicatif, article 7, paragraphe 1, du protocole et paragraphe 100 du rapport explicatif.
[47] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, STCE n° 108 (ci-après la «convention 108»).

[48] Voir à cet égard, avis 4/2001 du groupe de travail Article 29 concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité, du 22 mars 2001 (5001/01/FR/Final WP 41), p. 6: «les signataires devraient être invités à signer la convention 108 du Conseil de l'Europe». 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, appelé «convention 108+», n'est pas encore entré en vigueur. Il a été signé par 26 États membres et ratifié par 11 États membres – voir l'état des signatures et des ratifications de la convention 108 +: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures
[49] Andorre, Argentine, Canada, Israël, Japon, Royaume-Uni et Suisse.
[50] Paragraphe 220 du rapport explicatif.
[51] Sans préjudice des conditions et des motifs de refus dont dispose la partie requise (voir ci-dessous).
[52] Caractères gras ajoutés.
[53] Conformément à l'article 15 de la convention sur la cybercriminalité, «chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950),
et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et **qui doit intégrer le principe de la proportionnalité**.
2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers (caractères gras ajoutés).
[54] Paragraphe 231 du rapport explicatif.
[55] Soulignement ajouté.
[56] Voir article 2 à la section 4.3.1.
[57] Voir paragraphe 97 du rapport explicatif. Cela découle également de l'article 7, paragraphe 1, de l'article 8, paragraphe 1, et de l'article 9, paragraphe 1, qui utilisent l'expression «données spécifiées».
[58] Voir, par exemple, à cet égard:
- l'article 6, paragraphe 3, point c), l'article 7, paragraphe 1, et l'article 8, paragraphe 1, qui font référence à la nécessité des informations, et le rapport explicatif, en particulier les paragraphes 82, 84 et 97;
- l'article 8, paragraphe 129, du rapport explicatif, qui précise que le mécanisme utilisé pour contraindre le fournisseur de services à fournir les informations sera soumis aux dispositions du droit de la partie requise, étant donné que les procédures de la partie requise le contrôleront. «La Partie requise peut ainsi s'assurer que son propre droit, y compris les conditions en matière constitutionnelle et de droits de l'homme, est respecté, tout particulièrement pour ce qui est des éventuelles garanties supplémentaires, y compris celles qui sont nécessaires en matière de production des données relatives au trafic».
[59] Les conditions raisonnables du droit interne de la partie requise en vertu de l'article 6, paragraphe 2, et les conditions de l'article 9, paragraphe 6, qui prévoient en tout état de cause des demandes non contraignantes (voir également les paragraphes 77, 82 et 169 du rapport explicatif du protocole). En outre, en vertu de l'article 8, paragraphe 7, la partie requise peut préciser les conditions dans lesquelles elle pourrait se conformer à la demande. Voir également, à l'article 8, paragraphe 8, et à l'article 10, paragraphe 7, du protocole, la condition découlant de l'article 28, paragraphe 2, point b), de la convention sur la cybercriminalité (condition de ne pas utiliser les informations pour des enquêtes ou des procédures autres que celles mentionnées dans la demande) et de l'article 7, paragraphe 5, point c) ii), de l'article 8, paragraphe 8, et de l'article 10 du protocole (voir paragraphe 173 du rapport explicatif), les conditions découlant de l'article 25, paragraphe 4, de la convention sur la cybercriminalité, selon lesquelles l'entraide est soumise aux conditions prévues par le droit de la partie requise ou par les traités d'entraide judiciaire applicables.

[60] Le paragraphe 269 du rapport explicatif de la convention sur la cybercriminalité précise qu'en vertu de l'article 27, paragraphe 4, de la convention, «le refus d'entraide au motif de la protection des données ne peut être invoqué que dans des cas exceptionnels. Une telle situation pourrait se présenter lorsque, après avoir pesé les intérêts importants impliqués dans un cas particulier (d'une part les intérêts publics, y compris la bonne administration de la justice et, d'autre part, des intérêts liés à la vie privée), il apparaît que la communication des données spécifiées, recherchées par la Partie requérante, soulèverait des problèmes d'une telle ampleur que la Partie requise pourrait les considérer comme relevant de motifs de refus fondés sur ses intérêts essentiels. Une application large, catégorique ou systématique des principes de protection des données pour refuser la coopération n'est, par conséquent, pas permise. Ainsi, le fait que les Parties concernées disposent de systèmes différents de protection du caractère privé des données (par exemple, la Partie requérante ne dispose pas de l'équivalent d'une autorité spécialisée en matière de protection des données) ou emploient des moyens différents pour protéger les données à caractère personnel (par exemple, la Partie requérante utilise des moyens autres que la procédure de suppression des données pour protéger le caractère privé ou l'exactitude des données à caractère personnel reçues par les autorités chargées de l'application de la loi), ne constitue pas, en soi, un motif de refus. Avant d'invoquer les "intérêts essentiels" comme motif pour refuser la coopération, la Partie requise devrait, à la place, essayer de fixer des conditions qui permettraient le transfert des données» (accent ajouté). Ce motif de refus est disponible en vertu de:

- l'article 7, paragraphe 5, point c) ii) (coopération directe avec les fournisseurs de services pour la production d'informations relatives aux abonnés), à condition que la partie requise ait fait usage de la possibilité d'exiger la consultation de son autorité – ce que la Commission propose pour les États membres à l'annexe;

- l'article 8, paragraphe 8 (coopération entre les autorités pour la production accélérée de données relatives aux informations sur les abonnés et au trafic);
- l'article 10, paragraphe 7 (entraide urgente).

Voir, en outre, les motifs de refus prévus à l'article 7, paragraphe 5, point c) ii), à l'article 8, paragraphe 8, et à l'article 10 du protocole (voir paragraphe 173 du rapport explicatif), découlant de l'article 25, paragraphe 4, de la convention sur la cybercriminalité, selon lequel l'entraide est soumise aux conditions fixées par le droit interne de la partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la partie requise peut refuser la coopération.

[61] Caractères gras ajoutés.

[62] Pour ce qui concerne le principe de proportionnalité, voir section 4.2.

[63] Le paragraphe 221 du rapport explicatif précise que «chaque Partie est tenue de traiter les données à caractère personnel qu'elle reçoit en vertu du présent Protocole conformément aux garanties expressément prévues aux paragraphes 2 à 15. Sont également couvertes les données à caractère personnel transférées en exécution d'une injonction ou d'une demande faite en vertu du présent Protocole».

[64] Pour le partage ultérieur et les transferts ultérieurs, voir ci-dessous.

[65] Voir également les explications détaillées figurant dans le rapport explicatif sur ce qui pourrait constituer un but qui n'est pas incompatible, aux paragraphes 227 et suivants.

[66] Paragraphe 228. «Le cadre juridique d'une Partie peut fixer des limites particulières concernant d'autres objectifs pour lesquels les données peuvent être utilisées.».

[67] Article 13 et paragraphe 218 du rapport explicatif.

[68] Voir ci-dessus pour l'interprétation de la notion de «pertinent et non excessif».

[69] Conformément à l'article 3, paragraphe 1, point e), du protocole, «l'expression "Partie transférante" désigne la Partie qui transmet les données en réponse à une demande ou dans le cadre d'une équipe d'enquête commune, ou, aux fins de la section 2 du chapitre II, une Partie sur le territoire de laquelle se trouve un prestataire de services en mesure de transmettre ou une entité fournissant des services d'enregistrement de noms de domaine».

[70] Soulignement ajouté.

[71] Paragraphe 230 du rapport explicatif.

[72] Paragraphe 230.

[73] Article 6, paragraphe 3, point d), article 7, paragraphe 4, point f), article 8, paragraphe 3, et article 9, paragraphe 3, point g), paragraphes 84, 105, 106, 131, 135 et 165 du rapport explicatif, ainsi que l'article 10, paragraphe 7, lu conjointement avec l'article 27, paragraphe 3, de la convention sur la cybercriminalité.

[74] Article 6, paragraphe 3, point c), article 8, paragraphe 8, et article 10, paragraphe 7.

[75] Voir paragraphe 71.

[76] Paragraphe 111.

[77] Conformément à l'article 7, paragraphe 5, point d), les autorités informées de l'État requis peuvent demander, aux fins d'enjoindre au fournisseur de services de ne pas divulguer les informations relatives aux abonnés, des informations complémentaires à l'autorité de la partie requérante à laquelle le fournisseur de services doit transmettre les informations relatives à l'abonné ou y répondre d'une autre manière, et ne divulgueront pas les informations supplémentaires reçues au fournisseur de services sans le consentement de cette autorité. Elles doivent également informer rapidement ladite autorité que le fournisseur de services a reçu pour instruction de ne pas divulguer les informations relatives à l'abonné et elles doivent motiver cette décision.

[78] Paragraphe 71.

[79] Paragraphes 241 et 242.
[80] Paragraphe 234.
[81] Article 5, paragraphe 1, point f), du RGPD et article 4, paragraphe 1, point f), de la directive (UE) 2016/680.
[82] Paragraphes 246 et 247.
[83] Article 6, paragraphe 4, article 7, paragraphe 6, article 8, paragraphe 5, article 9, paragraphe 4, et article 10, paragraphe 2, et paragraphes 86, 116 et 174 du rapport explicatif.
[84] Paragraphe 258.
[85] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 141.
[86] Caractères italiques ajoutés.
[87] Caractères italiques ajoutés.
[88] Cela doit être lu en combinaison avec le principe de limitation de la finalité inscrit au chapitre II et à l'article 13 en ce qui concerne les informations demandées: voir, en particulier, la section 4.2 sur le principe de proportionnalité et la section 4.3.1 sur la limitation de la finalité et la minimisation des données ci-dessus.
[89] Paragraphe 248.
[90] Voir note de bas de page 59.
[91] Voir les sections sur les principes de proportionnalité, de limitation de la finalité et de minimisation des données ci-dessus.
[92] Voir les sections sur les principes de proportionnalité, de limitation de la finalité et de minimisation des données, en particulier la note de bas de page 60.
[93] Article 6, paragraphe 3, point d), article 7, paragraphe 4, point f), article 8, paragraphe 3, et article 9, paragraphe 3, point g), paragraphes 84, 105, 106, 131, 135 et 165 du rapport explicatif, ainsi que l'article 10, paragraphe 7, lu conjointement avec l'article 27, paragraphe 3, de la convention sur la cybercriminalité.
[94] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 141.
[95] Paragraphe 245.

[96] Voir également section 4.3.6.
[97] Voir ci-dessous.
[98] Paragraphe 111.
[99] Article 6, paragraphe 3, point d), article 7, paragraphe 4, point f), article 8, paragraphe 3, et article 9, paragraphe 3, point g), paragraphes 84, 105, 106, 131, 135 et 165 du rapport explicatif, ainsi que l'article 10, paragraphe 7, lu en combinaison avec l'article 27, paragraphe 3, de la convention sur la cybercriminalité.
[100] Voir affaire C-518/07, Commission/Allemagne, EU:C:2010:125, point 25; affaire C-288/12, Commission/Hongrie, EU:C:2014:237, point 48.
[101] Paragraphe 322.
[102] Article 7, paragraphe 5, point c) ii), article 8, paragraphe 8, et article 10, paragraphe 7.
[103] Article 6, paragraphe 2, et article 9, paragraphe 6.
[104] Article 25 – Principes généraux relatifs à l'entraide – paragraphe 4: «Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale». Les infractions visées aux articles 2 à 11 de la convention sont une liste des infractions portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques, des infractions liées à l'informatique et au contenu, des infractions liées aux atteintes au droit d'auteur et aux droits voisins, de la complicité dans la commission de ces infractions et de la tentative de commettre certaines autres infractions prévues par la convention.
Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables – paragraphe 4: «Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:
a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels».
[105] Conformément à l'article 3, paragraphe 2, point b), du protocole, «l'expression "autorité compétente" désigne une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par le présent Protocole aux fins du recueil ou de la production de preuves concernant des enquêtes ou procédures pénales spécifiques».
[106] Affaires jointes C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 120.
[107] Affaires jointes C-293/12 et C594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238, point 62.
[108] Article 5, paragraphe 6, du protocole et paragraphe 69 du rapport explicatif.
[109] Paragraphe 93 du rapport explicatif du protocole.
[110] Affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, point 99.
[111] Affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970, point 120.

[112] Affaire C-746/18, Prokuratuur, ECLI:EU:C:2021:152, dispositif de l'arrêt: «2) L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale».
[113] Affaire C-201/14, Smaranda Bara e.a./Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală, ECLI:EU:C:2015:638, point 33: «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 [...]».
[114] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 220.
[115] Article 14, paragraphe 11, point c), du protocole.
[116] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 219.
[117] Paragraphe 276 du rapport explicatif.
[118] Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650, point 95.
[119] Ibidem, point 95 (caractères gras ajoutés).
[120] Ibidem, points 56 à 58.
[121] Affaire C-518/07, Commission/Allemagne, ECLI:EU:C:2010:125, point 25; affaire C-614/10, Commission/Autriche, ECLI:EU:C:2012:631, points 36 et 37; et affaire C-288/12, Commission/Hongrie, point 48.
[122] Avis 1/15, accord PNR UE-Canada, ECLI:EU:C:2017:592, point 229.
[123] Paragraphes 278 et suivants.
[124] Paragraphes 281.

[125] Paragraphes 222.
[126] 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 du 10.12.2016, p. 3 (ci-après l'«accord-cadre»). L'accord-cadre 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.
[127] Voir la réponse conjointe de l'EDPB et du CEPD à la commission LIBE concernant l'incidence du Cloud Act sur le cadre juridique européen pour la protection des données à caractère personnel.
[128] Avis 7/2019 du CEPD concernant les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.
[129] Caractères italiques ajoutés.