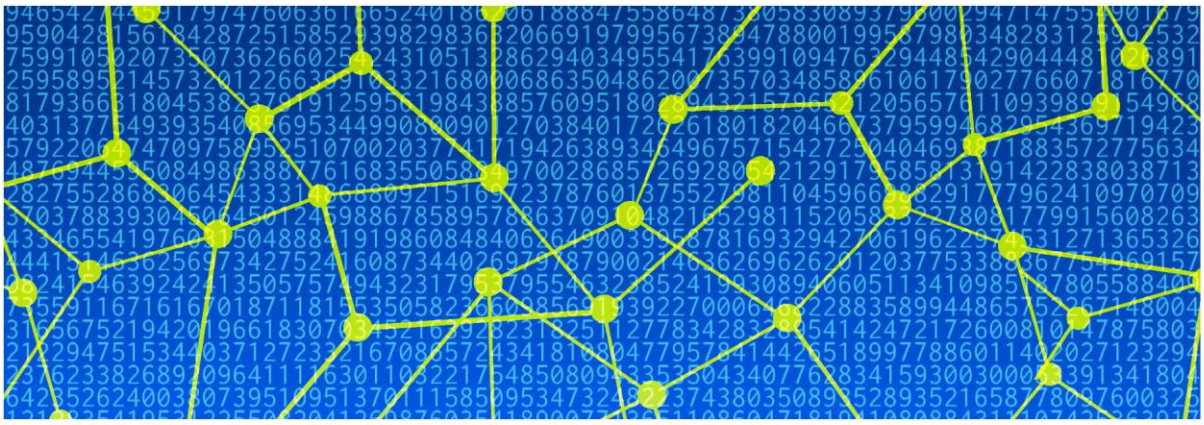

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 7/2019

Avis du CEPD concernant les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

EDPS

6 novembre 2019

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». En vertu de l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725, le CEPD dispose du pouvoir d'«émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public, sur toute question relative à la protection des données à caractère personnel».

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

Le présent avis se rapporte à la mission du CEPD de conseiller les institutions de l'Union sur les implications de leurs politiques en matière de protection des données et de promouvoir une élaboration responsable des politiques, conformément à l'action n° 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques». Le CEPD soutient l'objectif visant à rendre plus efficace l'accès transfrontière aux preuves électroniques, mais insiste sur la nécessité d'améliorer les propositions législatives présentées par la Commission afin de garantir le respect des droits fondamentaux et le respect des exigences en matière de protection des données. Ces deux éléments sont essentiels à la mise en place d'un cadre efficace pour les injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

Synthèse

En avril 2018, la Commission a présenté une proposition de règlement et une proposition de directive visant à établir un cadre juridique qui permettrait aux autorités policières et judiciaires de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement dans le cadre des affaires transfrontières. Depuis lors, le Conseil a adopté des orientations générales en la matière et le Parlement européen a publié plusieurs documents de travail. Le comité européen de la protection des données a rendu son avis. La situation a également évolué au niveau international, avec notamment l'ouverture de négociations en vue de parvenir à un accord international avec les États-Unis sur l'accès transfrontière aux preuves électroniques, ainsi que le lancement de travaux portant sur un deuxième protocole additionnel à la convention sur la cybercriminalité. Par le présent avis, le CEPD souhaite fournir au législateur de l'Union de nouvelles informations pour les travaux à venir sur les propositions, compte tenu de l'évolution susmentionnée.

Dans le monde d'aujourd'hui, transformé par les nouvelles technologies, le temps est souvent compté pour permettre à ces autorités d'obtenir les données indispensables à l'accomplissement de leurs missions. Parallèlement, même lorsqu'elles enquêtent sur des affaires internes, les autorités répressives rencontrent de plus en plus souvent des «questions transfrontières», tout simplement parce qu'un fournisseur de services étranger a été utilisé et que les informations sont stockées sous forme électronique dans un pays tiers. Le CEPD **soutient l'objectif** visant à garantir que les autorités répressives disposent d'outils efficaces pour enquêter sur les infractions pénales et en poursuivre leurs auteurs, et se félicite en particulier de l'objectif des propositions visant à accélérer et à faciliter l'accès aux données dans les affaires transfrontières en simplifiant les procédures dans l'Union.

Parallèlement, le CEPD tient à souligner que toute initiative dans ce domaine doit **respecter pleinement la charte des droits fondamentaux de l'Union européenne et le cadre de l'Union en matière de protection des données** et qu'il est essentiel de garantir l'**existence de toutes les garanties nécessaires**. En particulier, la protection efficace des droits fondamentaux dans le processus de collecte transfrontière des preuves électroniques exige une **plus grande participation des autorités judiciaires de l'État membre chargé de la mise en œuvre**. Elles devraient, dès que possible, être systématiquement associées à ce processus, avoir la possibilité de vérifier la conformité des injonctions avec la charte et être tenues d'invoquer les motifs de refus sur cette base.

En outre, les **définitions des catégories de données** figurant dans la proposition de règlement devraient être clarifiées et leur cohérence avec les autres définitions des catégories de données relevant du droit de l'Union devrait être assurée. Le CEPD recommande également de réévaluer l'équilibre entre les **types d'infractions** pour lesquelles des injonctions européennes de production pourraient être émises et les **catégories de données** concernées, en tenant compte de la jurisprudence pertinente de la Cour de justice de l'Union européenne.

En outre, le CEPD formule des recommandations spécifiques sur plusieurs aspects des propositions relatives aux preuves électroniques qui demandent d'être améliorés: l'**authenticité et la confidentialité des injonctions et des données transmises**, la **conservation limitée** au titre des injonctions européennes de conservation, le **cadre applicable en matière de protection des données**, les **droits des personnes concernées**, les personnes bénéficiant des **immunités et privilèges**, les **représentants légaux**, les **délais** de mise en œuvre des injonctions européennes de production et la **possibilité pour les fournisseurs de services** de s'y opposer.

Enfin, le CEPD demande plus de clarté sur l'interaction de la proposition de règlement avec les futurs accords internationaux. Le règlement proposé devrait maintenir le niveau élevé de protection des données dans l'Union et devenir une référence lors de la négociation d'accords internationaux sur l'accès transfrontière aux preuves électroniques.

TABLE DES MATIÈRES

1. INTRODUCTION ET CONTEXTE 6

2. OBJECTIFS DES PROPOSITIONS 7

3. RECOMMANDATIONS PRINCIPALES 9

3.1. DÉFINITIONS CLAIRES DES CATÉGORIES DE DONNÉES À CARACTÈRE PERSONNEL 9

3.2. TYPE D'INFRACTIONS CONCERNÉES 11

3.3. SÉCURITÉ DES DONNÉES 13

3.4. PARTICIPATION ACCRUE DES AUTORITÉS JUDICIAIRES DE L'ÉTAT MEMBRE CHARGÉ DE LA MISE EN ŒUVRE 15

3.5. CONSERVATION LIMITÉE EN VERTU D'INJONCTIONS EUROPÉENNES DE CONSERVATION 16

4. RECOMMANDATIONS COMPLÉMENTAIRES 17

4.1. RÉFÉRENCE COMPLÈTE AU CADRE APPLICABLE EN MATIÈRE DE PROTECTION DES DONNÉES 17

4.2. DROITS DES PERSONNES CONCERNÉES 18

4.3. PERSONNES CONCERNÉES BÉNÉFICIANT D'IMMUNITÉS ET DE PRIVILÈGES 19

4.4. REPRÉSENTANTS LÉGAUX 19

4.5. DÉLAIS DE PRODUCTION DES DONNÉES 20

4.6. POSSIBILITÉ POUR LES FOURNISSEURS DE SERVICES DE S'OPPOSER À UNE INJONCTION 21

4.7. INTERACTION AVEC D'AUTRES INSTRUMENTS 21

5. CONCLUSIONS 22

NOTES 25

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

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

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

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

vu 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)[2],

vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[3],

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. Le 17 avril 2018, la Commission a publié deux propositions législatives (ci-après les «propositions»), accompagnées d'une analyse d'impact[4], dont:
   - une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[5] (ci-après la «proposition de règlement»);
   - une proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale[6] (ci-après la «proposition de directive»).

2. Le règlement proposé coexisterait avec la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale (ci-après la «directive DEE»)[7], qui vise à faciliter la collecte de preuves sur le territoire d'un autre État membre et couvre tout type de collecte de preuves, y compris les données électroniques[8]. Tous les États membres qui ont participé à l'adoption de la directive DEE[9] avaient jusqu'en mai 2017 pour la transposer dans leur législation nationale[10].

3. Le 26 septembre 2018, le comité européen de la protection des données[11] (ci-après le «comité») a adopté un avis[12] sur les propositions.

4. Le 7 décembre 2018 et le 8 mars 2019, le Conseil a adopté son orientation générale sur la proposition de règlement[13] et la proposition de directive[14] respectivement. Le Parlement européen a publié une série de documents de travail.

5. Le CEPD se réjouit que les services de la Commission l'aient consulté de manière informelle avant l'adoption des propositions. Il se félicite également des références faites au présent avis au considérant 66 de la proposition de règlement et au considérant 24 de la proposition de directive.

6. Le 5 février 2019, la Commission a adopté deux recommandations relatives aux décisions du Conseil: une recommandation d'autoriser l'ouverture de négociations en vue d'un accord international entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale[15] et une recommandation d'autoriser la Commission, au nom de l'Union européenne, à participer aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (STCE nº 185) (ci-après la «convention sur la cybercriminalité»)[16]. Les deux recommandations ont fait l'objet de deux avis du CEPD[17]. Les négociations engagées avec les États-Unis et celles au sein du Conseil de l'Europe sont étroitement liées.

7. En février 2019, la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a adressé des lettres similaires au CEPD et au comité afin de demander une évaluation juridique de l'incidence de la loi américaine sur la surveillance des données à caractère personnel (le «Claryfing Lawful Overseas Use of Data Act» ou «CLOUD Act»)[18], adoptée par le Congrès américain en mars 2018, sur le cadre juridique européen en matière de protection des données. Le 12 juillet 2019, le CEPD et le comité ont adopté une réponse commune à cette demande, accompagnée de leur évaluation initiale[19].

8. Le 3 octobre 2019, le Royaume-Uni et les États-Unis ont signé un accord bilatéral sur l'accès transfrontière aux preuves électroniques aux fins de la lutte contre la grande criminalité[20]. Il s'agit du premier accord exécutif permettant aux fournisseurs de services des États-Unis de se conformer aux demandes de données sur le contenu provenant d'un pays étranger en vertu du CLOUD Act.

9. Le présent avis porte sur les deux propositions, l'accent étant toutefois mis sur la proposition de règlement. Conformément au mandat du CEPD, l'avis porte principalement sur les droits à la vie privée et à la protection des données à caractère personnel et tend à être cohérent et complémentaire par rapport à l'avis 23/2018 du comité, tout en tenant également compte des approches générales du Conseil et des documents de travail du Parlement européen.

2. OBJECTIFS DES PROPOSITIONS

10. L'objectif majeur de la proposition de règlement est d'accélérer la collecte et l'obtention de preuves électroniques par-delà des frontières[21]. À cette fin, il introduirait deux nouveaux types d'injonctions contraignantes: l'injonction européenne de production imposant à un fournisseur de services de produire des données et l'injonction européenne de conservation imposant à un fournisseur de services de conserver, en vue d'une demande ultérieure de production, des données qui pourront être utilisées comme preuves dans le cadre d'une procédure pénale.

11. Les mesures proposées impliqueraient le traitement de données à caractère personnel et des limitations au droit à la vie privée garanti par l'article 7[22] de la charte et au droit à la protection des données à caractère personnel garanti par l'article 8[23] de la charte. Pour être légale, toute limitation de l'exercice des droits fondamentaux protégés par la charte doit

respecter les critères énoncés à l'article 52, paragraphe 1, de ladite charte. Il s'agit, entre autres, de veiller à ce que toute limitation du droit à la protection des données à caractère personnel soit «nécessaire» et «proportionnée». Afin d'aider le législateur de l'Union à évaluer la conformité des mesures législatives proposées concernant le traitement des données à caractère personnel, le CEPD a publié un «Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel»[24] fondé sur la jurisprudence pertinente et ses avis antérieurs.

12. En vertu de la proposition de règlement, les injonctions ne seraient émises que dans des situations transfrontières[25] et non dans des situations nationales[26]. Les injonctions de production ne seraient émises ou validées par une autorité judiciaire d'un État membre que s'il existe une mesure similaire pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission. Les injonctions seraient directement émises par l'autorité d'émission aux fournisseurs de services proposant des services dans l'Union européenne (ci-après l'«Union»)[27] et établis ou représentés par un représentant légal dans un autre État membre. Elles seraient transmises aux fournisseurs de services au moyen de certificats d'injonction européenne de production (ci-après l'«EPOC») ou de certificats d'injonction européenne de conservation (ci-après l'«EPOC-PR»). Les injonctions seraient exécutées directement dans l'État membre chargé de la mise en œuvre, sans procédure préalable de reconnaissance et de mise en œuvre dans cet État membre. Toutefois, sous certaines conditions, des motifs limités pourraient être invoqués dans l'État membre chargé de la mise en œuvre pour s'opposer à la reconnaissance ou à la mise en œuvre des injonctions (article 14) ou pour demander dans l'État membre d'émission le réexamen d'une injonction européenne de production (articles 15 et 16).

13. La proposition de directive vise à élaborer une approche commune à l'échelle de l'Union permettant d'identifier les destinataires d'une EPOC ou d'une EPOC-PR[28]. À cette fin, elle impose à tous les fournisseurs de services proposant des services dans l'Union l'obligation de désigner un représentant légal dans l'Union[29], qui serait responsable de la réception de l'EPOC ou de l'EPOC-PR et de leur mise en œuvre complète et en temps utile[30].

14. À la lumière des difficultés rencontrées par les autorités policières et judiciaires pour rassembler des preuves électroniques dans le monde numérique actuel, qui ne connaît pas de frontières, **le CEPD soutient l'objectif de fournir aux autorités répressives des outils efficaces leur permettant d'accéder rapidement à des preuves électroniques par-delà les frontières. Dans de nombreux cas, il est essentiel d'agir rapidement afin que ces autorités puissent obtenir les données indispensables à leurs enquêtes et à leurs poursuites.** Même lorsqu'elles enquêtent sur des affaires internes, les autorités répressives rencontrent de plus en plus souvent des «questions transfrontières», tout simplement parce qu'un fournisseur de services étranger a été utilisé et que les informations sont stockées sous forme électronique dans un pays tiers. Par conséquent, **le CEPD se félicite que les propositions relatives aux preuves électroniques visent à accélérer et à faciliter cet accès dans les affaires transfrontières ainsi qu'à accroître la sécurité juridique grâce à une harmonisation des procédures au sein de l'Union**. Parallèlement, **il insiste sur la nécessité de veiller à ce que la conservation des preuves électroniques et l'accès à celles-ci respectent pleinement la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») et le cadre en matière de protection des données**.

15. Le CEPD constate que l'analyse d'impact accompagnant les propositions considère le droit à la liberté et à la sûreté consacré à l'article 6 de la charte comme «*les droits fondamentaux des personnes qui sont ou peuvent devenir victimes de la criminalité*[31]». Le CEPD souligne

que ce droit vise à protéger la liberté et la sûreté individuelles contre l'État. Il n'est pas question ici d'un droit garanti par l'État[32].

16. Afin de satisfaire aux conditions énoncées à l'article 52, paragraphe 1, de la charte, le CEPD rappelle que la CJUE a jugé que le législateur de l'Union devrait «*prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*»[33]. Les propositions constituent le dernier volet d'une série de mesures législatives par lesquelles le législateur de l'Union est appelé à concilier les droits des individus en matière de protection des données et l'intérêt général à combattre et à poursuivre les infractions pénales. De telles mesures sont évidemment susceptibles d'entrer en conflit avec les droits en matière de protection des données[34]. **Il est donc essentiel d'examiner attentivement ces propositions et d'accorder une attention particulière à l'existence de toutes les garanties nécessaires.**

3. RECOMMANDATIONS PRINCIPALES

3.1. Définitions claires des catégories de données à caractère personnel

17. Le terme «preuve électronique» est défini à l'article 2, point 6, de la proposition de règlement et est divisé en quatre sous-catégories: «données relatives aux abonnés», «données relatives à l'accès», «données relatives aux transactions» et «données relatives au contenu» définies respectivement à l'article 2, points 7, 8, 9 et 10. Cette division reflète la «nature sensible»[35] de chaque catégorie de données et, sur cette base, prévoit des exigences différentes[36] pour l'accès aux données relevant de ces catégories.

3.1.1. Définitions cohérentes des catégories de données dans le droit de l'Union

18. Le CEPD souligne l'importance de garantir la cohérence entre les définitions des catégories de données figurant dans la proposition de règlement et les autres définitions des catégories de données figurant dans le droit de l'Union. À cet égard, le CEPD constate que la proposition de règlement tient compte des définitions proposées dans le cadre de la proposition de règlement «vie privée et communications électroniques», qui définirait les données de communications électroniques[37] et distinguerait les deux catégories de données relatives au contenu de communications électroniques[38] et les métadonnées de communications électroniques[39].

19. Si la catégorie des données relatives au contenu figurant dans la proposition de règlement semble conforme à la catégorie des données relatives au contenu de communications électroniques figurant dans la proposition de règlement «vie privée et communications électroniques», les catégories des **données relatives aux transactions et des données relatives à l'accès figurant dans la proposition de règlement sont de nouvelles catégories de données**. Elles ne sont actuellement pas définies dans la législation de l'Union en matière de protection des données et elles couvrent toutes deux, sans toutefois s'y limiter, les métadonnées de communications électroniques telles qu'elles sont définies dans la proposition de règlement «vie privée et communications électroniques». Le futur règlement «vie privée et communications électroniques» s'appliquerait à la conservation et à la production des données des fournisseurs de services de communications électroniques dans

le cadre de la proposition de règlement relatif aux preuves électroniques. **Le CEPD estime qu'il est par conséquent essentiel de garantir une cohérence totale entre les définitions de ces deux textes tout au long du processus législatif. Le CEPD rappelle qu'il a demandé à plusieurs reprises l'adoption rapide du règlement «vie privée et communications électroniques» afin d'éviter toute insécurité juridique[40].**

3.1.2. Manque de clarté et chevauchement des catégories de données

20. Le CEPD souligne l'importance de formuler des définitions claires et simples de chaque catégorie de données afin de garantir la sécurité juridique pour toutes les parties concernées, ce qui est l'un des principaux objectifs de la proposition de règlement[41]. L'efficacité des injonctions pourrait être aisément compromise par un manque de précision et de clarté dans les définitions essentielles contenues dans la proposition de règlement.

21. Le règlement proposé introduirait une nouvelle catégorie des «données relatives à l'accès» définies comme «*les données relatives au début et à la fin d'une session d'accès utilisateur à un service*». L'article 2, point 8, définit également les données relatives à l'accès au regard de la finalité du traitement de ces données, à savoir qu'elles sont «*strictement nécessaires aux seules fins d'identification de l'utilisateur du service*». Il précise en outre qu'elles incluent également les métadonnées de communications électroniques. À la lecture de l'exposé des motifs, il apparaît qu'il est essentiel de couvrir cette catégorie des données relatives à l'accès, car ces données sont souvent, avec les données relatives aux abonnés, «*source d'indices utiles pour une enquête visant à identifier un suspect*»[42]. Le CEPD constate toutefois que cette nouvelle catégorie de données manque de cohérence avec les définitions existantes des catégories de données figurant dans le droit de l'Union et le droit des États membres[43]. La création de cette catégorie de données semble artificielle et a pour seul objectif d'imposer des exigences moins strictes à la production de telles données, analogues à celles qui s'appliquent à la production de données relatives aux abonnés (article 4, paragraphe 1). Par conséquent, le **CEPD recommande de réexaminer la nécessité d'introduire cette nouvelle catégorie des données relatives à l'accès**.

22. Par ailleurs, si le texte conserve la catégorie des données relatives à l'accès, le CEPD estime, tout comme le comité l'a déjà fait remarquer[44], que la définition proposée des données relatives à l'accès manque de clarté. Le CEPD fait observer que tant la définition des données relatives aux transactions que celle des données relatives à l'accès incluent les «métadonnées de communications électroniques» telles qu'elles sont définies dans la proposition de règlement «vie privée et communications électroniques». Elles citent toutes les deux, à titre d'exemples, un certain nombre de données relevant de leur catégorie. Certains exemples sont explicitement couverts par les deux définitions, comme la date et l'heure. En outre, la définition des données relatives aux transactions exclut les données relevant de cette catégorie si «*ces données constituent des données relatives à l'accès*». Dans la pratique, les fournisseurs de services peuvent avoir des difficultés à faire la distinction entre les données relatives à l'accès et les données relatives aux transactions, alors que la proposition de règlement prévoit que ces catégories doivent être produites dans des conditions différentes. Par conséquent, **le CEPD recommande de clarifier les définitions des données relatives à l'accès et des données relatives aux transactions et de délimiter clairement ces catégories afin de garantir la sécurité juridique. Les mêmes données ne devraient pas être produites dans des conditions différentes en fonction de la catégorie dans laquelle elles sont demandées. Dans le cas contraire, l'injonction européenne de production de données relatives à l'accès doit être soumise aux mêmes**

conditions que les données relatives aux transactions et les données relatives au contenu (article 4, paragraphe 2).

23. En outre, le CEPD partage des préoccupations similaires en ce qui concerne la catégorie des données relatives aux abonnés. La convention sur la cybercriminalité contient déjà une définition de l'expression «données relatives aux abonnés»[45], qui n'est pas toujours interprétée de manière uniforme par les parties à la convention[46]. La proposition de règlement donne la première définition de l'expression «données relatives aux abonnés» dans le droit de l'Union. Le CEPD estime que la définition de cette catégorie de données dans la proposition de règlement est un exercice difficile, mais important. Le CEPD souligne qu'il est essentiel d'éviter toute confusion entre les catégories des données relatives aux transactions et des données relatives aux abonnés, notamment en ce qui concerne l'article 2, paragraphe 7, point b), car la production de ces deux catégories de données serait également soumise à des conditions différentes. À cet égard, le CEPD souligne que les adresses IP pourraient entrer dans les deux catégories des données relatives aux transactions et des données relatives aux abonnés, en plus de la catégorie des données relatives à l'accès qui fait explicitement mention des adresses IP. **Le CEPD recommande de modifier la définition proposée pour les données relatives aux abonnés afin de mieux préciser cette catégorie, en particulier l'article 2, paragraphe 7, point b), et en ce qui concerne l'adresse IP, et d'éviter tout chevauchement avec d'autres catégories de données.**

3.2. Type d'infractions concernées

24. Le CEPD prend note du type d'infractions pour lesquelles les autorités peuvent émettre des injonctions européennes de production et de conservation. D'une part, l'injonction européenne de production ne peut être émise que si une mesure similaire est disponible pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission (article 5, paragraphe 2, de la proposition de règlement). Les injonctions européennes de production de données relatives aux abonnés ou de données relatives à l'accès peuvent être émises pour toutes les infractions pénales (article 5, paragraphe 3, de la proposition de règlement), tandis que les injonctions européennes de production de données relatives aux transactions ou de données relatives au contenu ne peuvent être émises que pour une série d'infractions énumérées à l'article 5, paragraphe 4, de la proposition de règlement:

    (a) toutes les «*infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins 3 ans*»; ou
    (b) les infractions «*si elles sont totalement ou partiellement commises au moyen d'un système d'information*» liées à la fraude et à la contrefaçon des moyens de paiement autres que les espèces, aux abus sexuels et à l'exploitation sexuelle des enfants, à la pédopornographie et aux attaques contre les systèmes d'information;
    (c) les infractions terroristes;

25. D'autre part, les injonctions européennes de conservation de données peuvent être émises pour toutes les infractions pénales sans distinction (article 6, paragraphe 2, de la proposition de règlement). L'exigence de disposer d'une mesure similaire pour les affaires nationales ne s'applique pas aux injonctions européennes de conservation.

26. Le CEPD estime que le seuil de peine privative de liberté maximale d'au moins trois ans proposé à l'article 5, paragraphe 4, point a), et la liste des infractions purement informatiques et des infractions facilitées par les technologies de l'information et de la

communication visées à l'article 5, paragraphe 4, point b), sont des points très problématiques, étant donné la nature sensible des données relatives aux transactions et des données relatives au contenu et la gravité de l'atteinte au droit à la vie privée et au respect des données qui en résulterait. Le seuil de peine privative de liberté maximale d'au moins trois ans proposé à l'article 5, paragraphe 4, point a), de la proposition de règlement s'appliquerait en pratique à un très grand nombre d'infractions prévues par les codes pénaux nationaux des États membres, parmi lesquelles de nombreuses infractions qui ne peuvent être considérées comme «graves»[47].

27. Le CEPD rappelle que la CJUE a conclu, à propos des métadonnées conservées par des fournisseurs de communications électroniques accessibles au public, que «*[c]es données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci*[48]» et «*fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications*[49]». En ce qui concerne les données relatives au contenu, la CJUE a estimé que l'accès à ces données peut même affecter l'essence même du droit à la vie privée et du droit à la protection des données[50].

28. En outre, le CEPD relève que la CJUE a jugé dans un arrêt qu'elle a récemment rendu dans l'affaire C-207/16 que «*conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de "grave"*» et que, dans ces domaines, «*seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont concernées*[51]». Le CEPD estime que l'accès des autorités nationales compétentes aux catégories des données relatives aux transactions et des données relatives au contenu permettrait de tirer des conclusions aussi précises concernant la vie privée des personnes dont les données seraient requises au moyen d'une injonction européenne de production. Par conséquent, il est essentiel que l'accès à ces catégories de données soit limité aux seuls cas de criminalité grave.

29. En ce qui concerne la liste des infractions purement informatiques et des infractions facilitées par les technologies de l'information et de la communication visées à l'article 5, paragraphe 4, point b), le CEPD n'est pas convaincu par la justification donnée au considérant 32 selon laquelle ces infractions sont «*des infractions spécifiques pour lesquelles les preuves sont généralement disponibles exclusivement sous forme électronique*» et «*l'application du même seuil que pour d'autres types d'infractions conduirait généralement à l'impunité*». Le CEPD estime que toutes les infractions purement informatiques et infractions facilitées par les technologies de l'information et de la communication énumérées à l'article 5, paragraphe 4, point b), ne peuvent pas constituer des «infractions graves». Reconnaissant toutefois qu'il pourrait être nécessaire et proportionné d'obtenir des données relatives aux transactions ou au contenu dans certains cas, le CEPD estime que ces données pourraient être obtenues grâce à la conservation de tout type de données au moyen d'une injonction européenne de production, avec une

demande de production des données conservées par l'intermédiaire des canaux traditionnels de coopération (tels qu'une décision d'enquête européenne), ce qui permettrait de maintenir les garanties élevées nécessaires.

30. **Pour ces raisons, le CEPD recommande de réévaluer l'équilibre entre les types d'infractions pour lesquelles des injonctions européennes de production pourraient être émises et les catégories de données concernées. En particulier, la possibilité d'émettre une injonction européenne de production de données relatives aux transactions et de données relatives au contenu devrait être limitée aux seules infractions graves[52].**

31. **En outre, compte tenu du caractère potentiellement révélateur des données relatives aux transactions et des données relatives au contenu, le CEPD estime que l'accès à ces données ne devrait être accordé que dans le contexte d'infractions graves spécifiques.** L'établissement d'une liste fermée de ces infractions graves permettrait également de renforcer la sécurité juridique pour toutes les parties concernées. Bien que la possibilité de limiter le champ d'application de l'injonction européenne de production à certaines infractions ait été écartée à un stade peu avancé de l'élaboration des propositions[53], le **CEPD recommande de réexaminer cette possibilité, en tenant compte de la jurisprudence pertinente de la CJUE[54].**

32. Enfin, le CEPD souligne que **des considérations similaires pourraient également s'appliquer aux injonctions européennes de production de données relatives aux abonnés et de données relatives à l'accès telles qu'elles sont actuellement définies dans la proposition de règlement, dans la mesure où ces catégories ne sont pas précisées et circonscrites et pourraient potentiellement inclure des «métadonnées» de communications électroniques**[55].

3.3. Sécurité des données

33. La législation européenne en matière de protection des données[56] impose clairement de garantir la sécurité des données à caractère personnel. La sécurité des données est également primordiale afin de garantir le secret des enquêtes et la confidentialité des procédures pénales. Tout en se félicitant de l'article 11 sur la confidentialité des informations et du considérant 57 de la proposition de règlement[57], le CEPD note que la proposition n'aborde pas de manière adéquate la question de l'authenticité des certificats reçus par les fournisseurs de services[58], de la sécurité de la transmission des données à caractère personnel aux autorités compétentes en réponse[59] et de la sécurité des injonctions reçues par les autorités chargées de la mise en œuvre[60].

34. Il est **primordial de vérifier l'authenticité des certificats et des injonctions** afin de veiller à ce que toutes les données à caractère personnel transmises restent confidentielles et d'éviter d'éventuelles violations de données susceptibles d'avoir des conséquences négatives pour les personnes concernées et d'engager la responsabilité des autorités chargées de la mise en œuvre, des fournisseurs de services ou de leurs représentants légaux en vertu des législations applicables en matière de protection des données. Par conséquent, **le CEPD recommande d'introduire dans la proposition de règlement des dispositions définissant la manière dont l'authenticité des certificats et des injonctions peut être garantie et vérifiée**. Le CEPD propose notamment d'étudier la possibilité d'utiliser des signatures numériques dans les cas où les injonctions et les certificats sont transmis par voie électronique. Afin d'atteindre l'objectif d'une collecte rapide des preuves

électroniques dans le respect des droits fondamentaux, le CEPD souligne qu'il est essentiel, de manière à garantir l'authenticité des documents, de veiller à ce que les moyens nécessaires soient mis en place pour que les données à caractère personnel soient divulguées et communiquées au titre des propositions dans un environnement sécurisé.

35. En ce qui concerne la **sécurité de la transmission des certificats et des données requises**, le CEPD se félicite que l'orientation générale du Conseil précise que l'EPOC et l'EPOC-PR doivent être transmis «*d'une manière sécurisée et fiable permettant au destinataire de produire une trace écrite et d'établir l'authenticité du certificat*»[61] et que les données requises doivent être «*transmises d'une manière sécurisée et fiable permettant d'établir l'authenticité et l'intégrité*»[62]. **Il estime toutefois que des garanties plus spécifiques et plus efficaces sont nécessaires, notamment en ce qui concerne la sécurité des injonctions reçues par les autorités chargées de la mise en œuvre**.

36. En ce qui concerne en particulier la **transmission des certificats**, l'article 8, paragraphe 2, de la proposition de règlement et de l'orientation générale du Conseil permettrait l'utilisation de plateformes spéciales ou de canaux sécurisés déjà établis pour le traitement des demandes par les autorités répressives et judiciaires. Toutefois, cette utilisation reste facultative et ne serait pas expressément autorisée pour d'autres communications par l'autorité émettrice impliquant des données à caractère personnel qui doivent avoir lieu après cette transmission.

37. Le CEPD note également que «*la Commission s'efforce de renforcer les mécanismes de coopération judiciaire existants à l'aide de mesures telles que la création d'une plateforme sûre pour échanger rapidement les demandes entre les autorités judiciaires au sein de l'UE*[63]» et qu'elle suggère d'envisager «*l'élargissement éventuel des plateformes e-CODEX*[64] *et SIRIUS*[65] *afin de mettre en place une connexion sécurisée avec les fournisseurs de services pour la transmission des EPOC et EPOC-PR ainsi que la réponse des fournisseurs, le cas échéant*»[66]. À cet égard, le CEPD observe qu'au cours des négociations au Conseil, un État membre a proposé «*l'ajout d'un nouveau considérant demandant à la Commission et aux États membres de travailler à la mise en place, dès que possible, de canaux de communication électroniques sécurisés permettant d'établir l'authenticité et l'intégrité*»[67]. À ce propos, le CEPD rappelle que toute mise en place d'un nouveau système informatique de traitement des données à caractère personnel requiert une base juridique et que, en particulier, du moins lorsque ce système informatique implique la participation d'une institution, d'un organe ou d'un organisme de l'Union, cette base juridique doit figurer dans un acte juridique de l'Union. **Par conséquent, le CEPD recommande de prévoir clairement dans le règlement une base juridique régissant explicitement l'utilisation d'un système informatique pour le traitement des données à caractère personnel aux fins du règlement**.

38. En outre, le CEPD se félicite que les propositions et l'orientation générale du Conseil[68] prévoient la publicité des informations relatives à l'**identification des autorités et des représentants légaux** des fournisseurs de services. Toutefois, **il recommande de modifier les propositions de manière à imposer ces obligations avant la date d'application d'autres dispositions, afin de garantir que toutes les informations requises soient disponibles à la date d'application des principales dispositions et d'éviter tout risque de violation de données à caractère personnel**[69].

3.4. Participation accrue des autorités judiciaires de l'État membre chargé de la mise en œuvre

39. Selon la proposition de règlement, le contrôle du respect des droits fondamentaux des personnes concernées par l'injonction européenne de production/conservation, y compris de la nécessité et de la proportionnalité des injonctions et l'applicabilité éventuelle des immunités et privilèges, serait principalement assuré par l'autorité d'émission. Les autorités compétentes de l'État membre chargé de la mise en œuvre n'interviendraient en tant qu'autorités chargées de la mise en œuvre que dans les cas où les fournisseurs de services ne respectent pas une injonction. Par conséquent, une fois les injonctions émises, étant donné que, dans la plupart des cas, les personnes concernées ne seraient pas immédiatement informées des injonctions[70], les fournisseurs de services seraient les seuls acteurs ayant la possibilité de protéger les droits au respect de la vie privée et à la protection des données des personnes concernées.

40. Selon l'approche traditionnelle en matière d'accès transfrontière aux preuves électroniques, il incombe prioritairement à l'État chargé de la mise en œuvre de garantir le contrôle de motifs limités de refus. Bien que le CEPD reconnaisse la nécessité de cerner d'autres approches en matière de collecte des preuves dans un contexte transfrontière, la nécessité de garanties efficaces à l'égard des droits fondamentaux des personnes concernées demeure de la plus haute importance. Il convient de tenir compte du fait que les législations applicables dans les États membres de l'Union, telles que celles portant sur la recevabilité des preuves collectées dans un autre État membre et sur ce qui constitue une infraction pénale, peuvent diverger[71]. Même dans le contexte de ces propositions, si elles sont adoptées, les conditions d'émission d'une injonction ne sont pas entièrement harmonisées dans l'ensemble de l'Union et des objections importantes, découlant du respect des droits fondamentaux, peuvent s'opposer à l'exécution d'une telle injonction[72]. Dans le contexte des négociations sur la directive DEE, l'Agence des droits fondamentaux a souligné que «*le respect des droits fondamentaux constitue une composante essentielle de l'espace de liberté, de sécurité et de justice, comme le prévoit l'article 67, paragraphe 1, du traité sur le fonctionnement de l'Union européenne: "L'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux et des différents systèmes et traditions juridiques des États membres"*[73]. *Ainsi, même si la reconnaissance mutuelle est présentée comme un "principe"*[74] *utilisé par les États membres de l'Union pour faciliter la coopération dans l'espace de liberté, de sécurité et de justice, les États membres doivent se conformer à leurs obligations légales de respecter les droits fondamentaux*»[75].

41. Le comité ne voit «*aucune justification à la procédure prévue dans le projet de règlement concernant les preuves électroniques permettant la production de données relatives au contenu sans la participation au moins des autorités compétentes de l'État membre dans lequel se trouve la personne concernée*»[76]. Le comité a également exprimé «*ses préoccupations quant à la suppression de tout double contrôle de l'injonction transmise par l'autorité compétente destinataire par rapport aux autres instruments*»[77]. Dans son orientation générale sur la proposition de règlement, le Conseil a introduit une notification aux autorités compétentes des États membres chargés de la mise en œuvre. Cette notification aurait lieu en même temps que l'envoi de l'EPOC aux fournisseurs de services. Toutefois, elle n'aurait pas d'effet suspensif. Elle aurait une portée limitée (elle ne serait requise pour l'EPOC concernant les données relatives au contenu[78] – qui sont les données les moins demandées[79] – que lorsque la personne concernée ne réside pas dans l'État membre d'émission). Enfin, les autorités notifiées ne pourraient soulever qu'un nombre limité de questions (aucun motif général de refus fondé sur les droits fondamentaux comme tels), sans

pouvoir empêcher directement l'exécution de la décision[80]. C'est la raison pour laquelle plusieurs États membres ont demandé que l'autorité notifiée soit investie d'un pouvoir plus important et qu'elle soit également habilitée à émettre des injonctions concernant des données non relatives au contenu[81].

42. **Le CEPD estime que, dans ce contexte, la protection effective des droits fondamentaux requiert un niveau de participation des autorités judiciaires de l'État membre chargé de la mise en œuvre. Par conséquent, il recommande d'associer systématiquement et aussi tôt que possible les autorités judiciaires désignées par l'État membre chargé de la mise en œuvre au processus de collecte de preuves électroniques afin de permettre à ces autorités de contrôler de manière efficace et efficiente la conformité des injonctions avec la charte et de garantir l'obligation pour ces autorités de soulever des motifs de refus sur cette base[82].**

43. En outre, la participation systématique des autorités judiciaires des États membres chargés de la mise en œuvre pourrait garantir le respect du principe de la double incrimination. Étant donné qu'il n'existe aucune harmonisation des infractions pénales dans l'Union, l'abandon du principe de double incrimination dans la proposition de règlement signifie que les données à caractère personnel peuvent être communiquées par un fournisseur de services aux fins de la poursuite d'un acte qui, selon la législation de l'État membre dans lequel il est établi, ne constitue pas une infraction pénale[83]. **Le CEPD estime que le principe de double incrimination est une garantie supplémentaire de protection des droits fondamentaux qui devrait figurer dans la proposition de règlement**. Comme le comité l'a déjà souligné[84], une telle garantie permettrait de «*s'assurer qu'un État ne peut pas s'appuyer sur l'assistance d'un autre État pour appliquer une sanction pénale qui n'existe pas dans la législation d'un autre État*»[85]. **Par conséquent, le CEPD recommande d'introduire l'exigence du principe de double incrimination dans la proposition de règlement, pour tous les cas dans lesquels des données sont requises sur la base d'une infraction qui n'est ni définie au niveau de l'Union ni convenue au niveau de l'Union dans une liste fermée à insérer dans le règlement**[86].

44. **Enfin, la participation des autorités judiciaires de l'État chargé de la mise en œuvre serait également plus conforme au choix de l'article 82, paragraphe 1, du traité FUE comme base juridique du règlement proposé.** Le CEPD note en effet que, jusqu'à présent, cet article n'a été utilisé que pour établir un mécanisme de coopération entre les autorités judiciaires. Conformément à ses avis 2/2019 et 3/2019[87], le CEPD doute fortement que cette disposition puisse servir de base juridique à l'adoption d'un règlement de l'Union établissant une coopération transfrontière directe entre les autorités judiciaires et les fournisseurs de services en matière pénale sans, en principe, la participation d'aucune autorité de l'État membre chargé de la mise en œuvre[88].

3.5. Conservation limitée en vertu d'injonctions européennes de conservation

45. Le règlement proposé établirait l'injonction européenne de conservation afin d'obliger les fournisseurs de services à conserver les données en vue d'une demande ultérieure de production de ces données au moyen d'une demande d'entraide judiciaire, d'une décision d'enquête européenne ou d'une injonction européenne de production. Ces injonctions visent à «*empêcher l'effacement, la suppression ou la modification des données concernées lorsque leur production risque de prendre plus de temps*»[89]. Le CEPD croit comprendre que l'injonction européenne de conservation concerne des données spécifiques stockées par le fournisseur de services au moment de la réception de l'EPOC-RP et ne concerne pas des

données futures stockées après cette date. Il est également important de souligner que l'injonction européenne de conservation n'établirait pas d'obligation générale de conservation des données[90].

46. Le CEPD rappelle le principe de la limitation de la conservation des données[91] selon lequel les données à caractère personnel sont conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La proposition de règlement prévoit que la conservation doit être limitée à un maximum de 60 jours «*à moins que l'autorité d'émission ne confirme que la demande de production suivante a été introduite*» (article 10, paragraphe 1). Si l'autorité d'émission procède à une telle confirmation au cours de la période de 60 jours, le destinataire continue à conserver les données aussi longtemps que nécessaire pour permettre leur production (article 10, paragraphe 2). Le considérant 42 précise que cette période de 60 jours a été calculée pour permettre l'introduction d'une demande officielle et qu'une telle «introduction» exige que quelques mesures formelles au moins aient été prises, par exemple, l'envoi d'une demande d'entraide judiciaire pour la traduction. Si la conservation des données n'est plus nécessaire, l'autorité d'émission doit en informer le destinataire sans retard injustifié (article 10, paragraphe 3). **Le CEPD croit comprendre que chaque injonction de conservation devrait en principe être liée à une demande ultérieure de production. Par conséquent, la durée de conservation des données requises est également liée à l'avenir de cette demande ultérieure. Le CEPD suggère dès lors de préciser que la conservation ne serait plus nécessaire et devrait cesser si la demande ultérieure est rejetée ou retirée.** Cette précision vaut également pour l'article 9, paragraphe 6, dernière phrase[92].

47. En outre, comme le comité l'a déjà souligné[93], l'injonction européenne de conservation ne devrait «*jamais servir de base permettant au fournisseur de services de traiter les données après la date initiale de leur suppression*». Le CEPD croit également comprendre que **les données conservées ne devraient pas être modifiées à compter de la réception de l'EPOC-PR et jusqu'à leur production à la suite d'une demande ultérieure de production**. Par conséquent, **le CEPD recommande de préciser davantage dans la proposition de règlement que les données requises dans le cadre d'une injonction européenne de conservation devraient être conservées et que leur traitement devrait être limité à leur stockage jusqu'à leur production.**

4. RECOMMANDATIONS COMPLÉMENTAIRES

4.1. Référence complète au cadre applicable en matière de protection des données

48. Le CEPD se félicite que la proposition de règlement tienne compte du cadre de l'Union en matière de protection des données et indique que les données à caractère personnel ne peuvent être traitées qu'en conformité avec le RGPD et la directive relative à la protection des données dans le domaine répressif (considérant 56 de la proposition de règlement). **Le CEPD recommande d'ajouter une référence à la directive 2002/58/CE «vie privée et communications électroniques» (qui sera remplacée par la proposition de règlement «vie privée et communications électroniques», une fois adoptée[94])**.

49. Le CEPD note que dans son orientation générale, le Conseil a ajouté une disposition sur le transfert ultérieur des données reçues par les autorités des États membres aux autorités d'États tiers dans les conditions prévues dans la proposition de règlement et au chapitre V de la directive (UE) 2016/680[95]. Le CEPD rappelle qu'en vertu de l'article 35 de la

directive (UE) 2016/680, un transfert de données à caractère personnel vers un pays tiers est soumis non seulement aux conditions définies au chapitre V, mais aussi au respect des dispositions nationales adoptées en application d'autres dispositions de ladite directive. **Par conséquent, le CEPD recommande de ne pas inclure une telle disposition dans le texte final**.

4.2. Droits des personnes concernées

4.2.1. Transparence accrue

50. Le CEPD estime qu'une connaissance générale de la fréquence et du volume des injonctions de conservation et de production adressées aux fournisseurs de services permettrait aux citoyens en général, mais également aux organismes publics, de comparer et d'évaluer la pratique générale dans l'utilisation de ces instruments. La transparence peut donc jouer un rôle important pour contribuer à garantir le respect des droits fondamentaux. Le CEPD note que certains fournisseurs de services[96] publient déjà régulièrement des rapports sur la transparence dans lesquels ils indiquent le nombre total de demandes d'accès reçues des autorités publiques et de réponses réservées à ces demandes.

51. **Par conséquent, le CEPD propose d'introduire l'obligation de publier périodiquement et sous une forme agrégée le nombre d'injonctions européennes de production et de conservation reçues par les fournisseurs de services au titre du règlement proposé, et d'indiquer si ces demandes ont été satisfaites ou non**[97].

4.2.2. Droit à un recours

52. Le CEPD se félicite de l'article 17 de la proposition de règlement, qui précise que les personnes concernées dont les données ont été obtenues ont droit aux recours disponibles en vertu du RGPD et de la directive relative à la protection des données dans le domaine répressif. **Il recommande d'ajouter le cas où les données ont été conservées** (étant donné qu'il ne peut être exclu qu'une violation des obligations en matière de protection des données se produise en relation avec ces données).

53. Les conditions de recours contre les fournisseurs de services pour violation des dispositions relatives à la protection des données en vertu du droit de l'Union en tant que responsables du traitement ou sous-traitants sont déjà prévues par le RGPD. Par exemple, en vertu de l'article 82, paragraphe 3, du RGPD, «*[u]n responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable*».

54. Le considérant 46 de la proposition de règlement dispose que «*[n]onobstant leurs obligations en matière de protection des données, les fournisseurs de services ne peuvent pas être tenus responsables dans les États membres des préjudices causés à leurs utilisateurs ou à des tiers résultant exclusivement de la conformité de bonne foi à un EPOC ou un EPOC-PR*». **Le CEPD estime qu'un instrument relatif à la coopération en matière pénale ne devrait pas modifier les conditions de responsabilité des responsables du traitement ou des sous-traitants (c'est-à-dire les fournisseurs de services ou les autorités compétentes) en vertu de la législation relative à la protection des données. Il convient par conséquent de supprimer le considérant 46**.

4.3. Personnes concernées bénéficiant d'immunités et de privilèges

55. Le CEPD se félicite de l'article 5, paragraphe 7, de la proposition de règlement en vertu duquel une injonction européenne de production de données relatives à l'accès, aux transactions ou au contenu ne devrait pas être émise si l'autorité d'émission constate que les données sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre dans lequel le fournisseur de services serait destinataire[98]. Il regrette que, selon l'orientation générale du Conseil, l'obligation de l'autorité d'émission de tenir compte des immunités et privilèges et, le cas échéant, de ne pas délivrer ou adapter une injonction européenne de production a été limitée aux seules situations dans lesquelles les immunités et les privilèges accordés en vertu de la législation des États chargés de la mise en œuvre concernent des données relatives aux transactions et dans lesquelles la «personne dont les données sont requises» ne réside pas sur le territoire de l'État membre d'émission[99].

56. En outre, l'autorité d'émission pourrait raisonnablement ne pas avoir connaissance des immunités ou des privilèges accordés en vertu de la législation de l'État membre chargé de la mise en œuvre. Par conséquent, le CEPD se félicite que, si une injonction européenne de production a été émise en dépit de ces immunités et privilèges accordés en vertu de la législation de l'État chargé de la mise en œuvre, l'article 14, paragraphe 2, de la proposition de règlement autorise l'autorité chargée de la mise en œuvre à refuser l'exécution d'une injonction, sans limitation quant aux données concernées[100]. Le CEPD note toutefois que ce n'est que dans les cas où, pour une autre raison, le certificat n'aurait pas été respecté par le fournisseur de services que l'autorité chargée de la mise en œuvre pourrait formuler une telle objection[101]. Selon l'orientation générale du Conseil, cette objection a été limitée aux cas où la «personne dont les données sont requises» ne réside pas dans l'État d'émission et aux données relatives au contenu[102].

57. Le CEPD prend également note de l'article 18 de la proposition de règlement[103] qui dispose que si des données sont obtenues en dépit de ces immunités et privilèges, «*ces motifs sont pris en considération de la même manière que s'ils avaient été prévus par sa législation nationale [...]*»[104].

58. Le CEPD **recommande de modifier la proposition de règlement afin de garantir au moins les points suivants:**
    - **une injonction européenne de production ne peut être émise si les données relatives aux transactions et les données relatives au contenu sont protégées par des immunités et des privilèges en vertu de la législation de l'État membre chargé de la mise en œuvre et qu'il n'a pas été possible d'obtenir la levée de ces immunités et privilèges[105];**
    - **l'État chargé de la mise en œuvre a l'obligation d'examiner ce motif pour toutes ces données[106].**

4.4. Représentants légaux

59. Comme l'a déjà souligné le comité[107], il convient d'éviter toute confusion entre les représentants légaux désignés par les fournisseurs de services proposant des services dans l'Union aux fins de la collecte de preuves dans le cadre de procédures pénales et les représentants désignés pour se conformer à l'article 27 du RGPD. De même, il convient

d'éviter toute confusion avec les représentants qui devraient être désignés pour se conformer à la proposition de règlement «vie privée et communications électroniques»[108].

60. Les représentants désignés pour se conformer à la directive proposée et au RGPD peuvent présenter certaines similitudes puisqu'ils feraient office de points de contact des fournisseurs de services qu'ils représentent. Ils auraient toutefois des tâches et des responsabilités très différentes par nature et ils répondraient à différents types de parties prenantes[109]. Ces deux fonctions exigent des connaissances et des compétences différentes. En outre, ces obligations de désigner des représentants peuvent s'appliquer à différents fournisseurs de services, selon qu'ils sont soumis ou non à la directive proposée ou au RGPD[110]. Par conséquent, **le CEPD recommande de préciser que ces différents types de représentants poursuivraient des objectifs différents et auraient des tâches et des responsabilités différentes**.

4.5. Délais de production des données

61. L'un des principaux objectifs de la proposition de règlement est d'accélérer la procédure transfrontière d'obtention de preuves dans un autre État par rapport aux mécanismes de coopération existants. Le CEPD note que les délais prévus par la proposition de règlement ne sont pas seulement un délai pour garantir une conservation et une production rapides des données, mais aussi un délai dans lequel le contrôle de conformité des certificats avec les droits fondamentaux, entre autres motifs, doit être effectué.

62. Tout en comprenant les objectifs de la proposition de règlement (tels que la prévention de la volatilité des données ou la garantie de l'efficacité des procédures pénales), le CEPD estime que les délais prévus dans tous les affaires[111] sont trop courts pour évaluer correctement les certificats reçus et déterminer s'il y a des raisons de ne pas les exécuter (par exemple une violation de la charte ou un conflit de législations) et prendre la décision appropriée. Le CEPD note que, à titre de comparaison, la directive DEE prévoit un délai de 30 jours pour que les autorités judiciaires de l'État chargé de la mise en œuvre puissent procéder à leur évaluation et décider de la «*reconnaissance ou exécution*» d'une décision d'enquête européenne[112] et de 90 jours suivant la date à laquelle la décision d'exécuter la mesure d'enquête a été prise[113]. Il souligne également qu'en tout état de cause, afin d'éviter la suppression des données requises lors de l'évaluation de l'EPOC, l'article 9, paragraphe 6, impose au fournisseur de services de «*conserve[r] les données demandées s'il ne l'est produit pas immédiatement*» et «*[l]es données sont conservées jusqu'à leur production*».

63. Par conséquent, **le CEPD recommande de fixer des délais supérieurs à dix jours, ce qui permettrait de procéder à une évaluation appropriée du certificat ainsi que de transmettre les données requises en temps utile**.

64. En outre, le CEPD note que, en dehors des cas d'urgence, la proposition de règlement autorise dans tous les cas les autorités d'émission à définir des délais inférieurs à 10 jours si elles indiquent «*les raisons d'une divulgation anticipée*». À moins qu'une justification supplémentaire ne soit fournie pour permettre aux autorités d'émission de se définir des délais plus courts dans tous les cas et de déroger aux délais prévus par la directive DEE, **le CEPD recommande de supprimer cette possibilité pour les autorités d'émission d'imposer aux fournisseurs de services des délais obligatoires plus courts que ceux prévus dans la proposition de règlement**.

65. Enfin, le CEPD estime que le délai de six heures fixé pour la production des données dans les cas d'urgence n'est pas toujours réaliste et **recommande d'en faire un délai de préférence plutôt qu'un délai obligatoire**.

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

66. Le CEPD se félicite que la proposition de règlement permette aux fournisseurs de services de s'opposer à la mise en œuvre d'une injonction. De telles objections devraient toutefois être fondées sur des motifs limités. Ces motifs devraient être clairement définis de manière à ce que les fournisseurs de services ne puissent décider, au cas par cas, d'accepter ou de refuser de coopérer, ou des modalités de cette coopération. À cet égard, le CEPD recommande en particulier d'introduire un motif d'opposition à l'exécution d'un EPOC (article 9) et à la mise en œuvre d'une injonction européenne de production (article 14) lorsque les données sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre chargé de la mise en œuvre (voir la section 4.3). Le CEPD note que les fournisseurs de services ne sont pas tenus d'évaluer ces motifs avant de mettre en œuvre l'injonction, mais qu'ils ne «peuvent s'opposer» à la mise en œuvre d'une injonction que sur cette base (article 14, paragraphes 4 et 5). Le CEPD pourrait soutenir une telle approche si, en revanche, un véritable mécanisme d'examen par les autorités d'un autre État membre que l'État d'émission était mis en place (voir la section 3.4). En particulier, le CEPD craint que le fait de soumettre les fournisseurs de services à d'éventuelles sanctions pécuniaires en cas de non-respect de leurs obligations, notamment de conserver ou de transmettre les données dès réception des certificats[114], ne les dissuade en réalité de soulever des objections dans des cas spécifiques[115].

4.7. Interaction avec d'autres instruments

67. Le CEPD note que le champ d'application de la proposition de règlement est défini de telle sorte qu'il permettrait en principe aux autorités compétentes dans l'Union de collecter des données auprès d'un fournisseur de services établi dans un pays tiers, quel que soit le lieu où se trouvent les données requises, pour autant qu'il propose ses services dans l'Union. Par conséquent, le fournisseur de services ou le traitement de ces données peut relever de la juridiction d'un pays tiers, ce qui peut entraîner des obligations contradictoires pour les fournisseurs de services découlant de la législation de l'Union, d'une part, et de celle d'un pays tiers, d'autre part. Par exemple, la loi des États-Unis sur les communications stockées (Stored Communications Act) interdit en principe la divulgation, par un fournisseur de services de communications électroniques[116] sous juridiction américaine, de données relatives au contenu à la suite de demandes émanant d'autorités étrangères, sauf si ces demandes émanent d'autorités de gouvernements étrangers qualifiés ayant conclu un accord exécutif avec les États-Unis[117] et si les données concernent des personnes non ressortissantes des États-Unis.

68. La Commission a cherché à traiter cette question en prévoyant dans la proposition de règlement une procédure de réexamen établissant un dialogue avec les autorités du pays tiers concerné en cas d'obligations contradictoires basées sur les droits fondamentaux (article 15), afin de servir d'exemple aux législateurs étrangers lorsque ces derniers élaborent leurs propres législations[118]. Parallèlement, la Commission a émis des recommandations de décisions du Conseil en vue de l'ouverture de négociations avec les États-Unis sur un accord international et l'autorisation de négocier, au nom de l'Union, le deuxième protocole additionnel à la convention sur la cybercriminalité (voir section 1). En mai 2019, le Conseil a adopté les décisions[119]. Les directives de négociation d'un accord

entre l'Union européenne et les États-Unis fixent des objectifs spécifiques, parmi lesquels «*prévenir les conflits de lois*» et «*fixer des règles communes pour les injonctions concernant l'obtention de preuves électroniques sous la forme de données relatives ou non relatives au contenu, adressées par une autorité judiciaire établie au sein d'une partie contractante à un fournisseur de services soumis au droit de l'autre partie contractante*[120]». Les directives de négociation du deuxième protocole additionnel à la convention sur la cybercriminalité prévoient que le protocole devrait comporter «*une clause [...] permettant aux États membres de continuer à appliquer les règles de l'Union européenne dans leurs relations mutuelles, plutôt que le deuxième protocole additionnel*[121]». Toutefois, à ce stade, il n'est pas encore clair sur la base de quels critères la distinction entre les affaires transfrontières au sein de l'Union (c'est-à-dire les affaires relevant du champ d'application des propositions) et affaires internationales (c'est-à-dire les affaires couvertes par un accord international) sera définie. À cet égard, le CEPD prend note de la disposition introduite par le Conseil dans son orientation générale (article 23)[122]. **Le CEPD recommande toutefois d'apporter plus de clarté sur cette question afin de garantir la sécurité juridique.** Ce point est important pour la légalité de tout traitement de données à caractère personnel dans ce contexte.

69. Le CEPD rappelle également que, en ce qui concerne la protection des données, la communication de données à caractère personnel aux autorités de pays tiers 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, ne peut avoir lieu que conformément aux règles en matière de transfert prévues au chapitre V de la directive relative à la protection des données dans le domaine répressif en l'absence d'accords internationaux applicables à l'obtention de preuves en matière pénale entre l'État membre et le pays tiers concerné. D'une manière générale, **le CEPD souligne l'importance de veiller à ce que le texte final du règlement proposé maintienne le niveau élevé de protection des données dans l'Union** afin que, lors de la négociation de tout accord international en matière d'accès transfrontière aux preuves électroniques, **il constitue une référence garantissant le respect des droits fondamentaux, dont les droits au respect de la vie privée et à la protection des données, et offrant des garanties solides.**

5. CONCLUSIONS

70. Le CEPD **soutient l'objectif** visant à garantir que les autorités répressives et judiciaires disposent d'outils efficaces pour enquêter sur les infractions pénales commises dans un monde transformé par les nouvelles technologies et en poursuivre les auteurs. Parallèlement, le CEPD souhaite s'assurer que cette mesure est pleinement respectueuse de la charte et de l'acquis de l'Union en matière de protection des données. Le règlement proposé exigerait le stockage et la communication de données à caractère personnel, tant à l'intérieur qu'à l'extérieur de l'Union, entre les autorités compétentes des États membres, les entités privées et, dans certains cas, les autorités de pays tiers. Il entraînerait des limitations aux deux droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la charte. Pour être licites, ces limitations doivent respecter les conditions prévues à l'article 52, paragraphe 1, de la charte et satisfaire notamment à la condition de nécessité.

71. D'une part, le CEPD estime que d'autres **solutions** qui offriraient de meilleures garanties, tout en réalisant les mêmes objectifs, devraient faire l'objet d'une évaluation plus approfondie.

72. Deuxièmement, le CEPD note que la proposition de règlement comprend déjà un certain nombre de garanties procédurales. Le CEPD est toutefois préoccupé par le fait que l'importante responsabilité d'examiner la conformité de l'EPOC et de l'EPOC-PR avec la charte est confiée aux fournisseurs de services et recommande d'**associer aussi tôt que possible les autorités judiciaires désignées par l'État membre chargé de la mise en œuvre** au processus de collecte des preuves électroniques.

73. Le CEPD recommande de garantir une plus grande cohérence entre les définitions des catégories de données de preuves électroniques et les **définitions de catégories spécifiques de données** relevant du droit de l'Union et de **réexaminer la catégorie des données relatives à l'accès,** ou de soumettre l'accès à ces données à des conditions analogues à celles qui s'appliquent aux catégories de données relatives aux transactions et de données relatives au contenu. La proposition de règlement devrait établir des définitions claires et simples de chaque catégorie de données afin de garantir la sécurité juridique pour toutes les parties concernées. Il recommande également de **modifier la définition proposée pour la catégorie des données relatives aux abonnés** afin de la préciser davantage.

74. De même, il recommande de **réévaluer l'équilibre entre le type d'infractions pour lesquelles des injonctions européennes de production pourraient être émises et les catégories de données concernées**, en tenant compte de la jurisprudence pertinente récente de la CJUE. En particulier, la possibilité d'émettre une injonction européenne de production de données relatives aux transactions et de données relatives au contenu devrait être limitée aux infractions graves. Idéalement, le CEPD serait favorable à la définition d'une liste fermée d'infractions pénales graves spécifiques pour les injonctions européennes de production de données relatives aux transactions et de données relatives au contenu, ce qui permettra également de renforcer la sécurité juridique pour toutes les parties concernées.

75. Le CEPD formule également des recommandations visant à garantir le respect des droits à la protection des données et au respect de la vie privée, tout en assurant une collecte rapide des preuves aux fins de procédures pénales spécifiques. Les recommandations portent en particulier sur la **sécurité de la transmission** des données entre toutes les parties concernées, l'**authenticité** des injonctions et des certificats et la **conservation limitée** des données dans le cadre d'une injonction européenne de conservation.

76. En plus des observations générales et des recommandations majeures susmentionnées, le CEPD formule des recommandations complémentaires concernant les aspects suivants des propositions:
    - la **référence au cadre applicable en matière de protection des données**;
    - les **droits des personnes concernées** (transparence accrue et droit à un recours légal);
    - les personnes concernées bénéficiant d'**immunités et privilèges**;
    - la **désignation de représentants légaux** pour la collecte de preuves en matière pénale;
    - les **délais requis pour se conformer** à un EPOC et produire les données;
    - la possibilité pour les **fournisseurs de services de s'opposer aux injonctions sur la base de motifs limités**.

77. Enfin, le CEPD est conscient du **contexte plus large** dans lequel l'initiative a été présentée et des deux décisions du Conseil adoptées, l'une concernant le deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe et l'autre portant sur l'ouverture de négociations avec les États-Unis. Il demande plus de clarté sur

l'interaction du règlement proposé avec les accords internationaux. Le CEPD souhaite vivement apporter une contribution constructive afin de garantir la cohérence et la compatibilité entre les textes finaux et le cadre de l'Union en matière de protection des données.

Fait à Bruxelles, le 6 novembre 2019

Wojciech Rafał WIEWIÓROWSKI
Contrôleur adjoint

NOTES

[1] JO L 295 du 21.11.2018, p. 39.
[2] JO L 119 du 4.5.2016, p. 1 (ci-après le «RGPD»).
[3] JO L 119 du 4.5.2016, p. 89 (ci-après la «directive relative à la protection des données dans le domaine répressif»).
[4] Document de travail des services de la Commission: Analyse d'impact, SWD(2018) 118 final (ci-après l'«analyse d'impact»), disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN.
[5] Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final.
[6] Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM(2018) 226 final.
[7] Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1; voir l'article 23 de la proposition de règlement).
[8] La directive DEE prévoit une coopération directe entre l'autorité d'émission d'un État membre et l'autorité d'exécution d'un autre État membre ou, le cas échéant, par l'intermédiaire de l'(des) autorité(s) centrale(s) désignée(s) par le(s) État(s) membre(s) concerné(s). Elle vise à faciliter et à accélérer cette coopération en prévoyant des formulaires normalisés et des délais stricts et en supprimant plusieurs obstacles à la coopération transfrontière. Par exemple, «*[l']autorité d'émission peut émettre une décision d'enquête européenne afin de prendre toute mesure visant à empêcher provisoirement toute opération de destruction, de transformation, de déplacement, de transfert ou d'aliénation d'éléments susceptibles d'être utilisés comme preuve*» et «*[l']autorité d'exécution se prononce sur la mesure provisoire et communique sa décision dans les meilleurs délais et, si possible, dans les 24 heures à compter de la réception de la décision d'enquête européenne*» (article 32). De même, l'exécution d'une décision d'enquête européenne aux fins de l'identification d'abonnés titulaires d'un numéro de téléphone ou de personnes détentrices d'une adresse IP spécifique n'est pas soumise à la condition de la double incrimination [article 10, paragraphe 2, point e), lu conjointement avec l'article 11, paragraphe 2]).
[9] Tous les États membres de l'Union, à l'exception du Danemark et de l'Irlande.
[10] Tous les États membres participants ont transposé la directive DEE dans leur législation nationale en 2017 ou en 2018. Voir l'état d'avancement de la mise en œuvre du réseau judiciaire européen: https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120.
[11] Institué par l'article 68 du RGPD, le comité a succédé au groupe de travail institué par l'article 29 de la directive 95/46/CE, qui a été abrogée. À l'instar du groupe de travail «article 29», le comité se compose de représentants des autorités nationales chargées de la protection des données et du CEPD.
[12] Avis 23/2018 du 26 septembre 2018 concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale [article 70, paragraphe 1, point b)](ci-après l'«avis 23/2018 du comité»), disponible à l'adresse suivante: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2018-09-26-eevidence_fr.pdf.
[13]https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#.
[14] https://www.consilium.europa.eu/fr/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/
[15] Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques à des fins de coopération judiciaire en matière pénale, COM(2019) 70 final.
[16] Recommandation de décision du Conseil autorisant la participation aux négociations sur un deuxième protocole additionnel à la convention sur la cybercriminalité du Conseil de l'Europe (SCTE nº 185), COM(2019) 71 final. À ce jour, tous les États membres de l'Union ont signé la convention du Conseil de l'Europe sur le renforcement de la coopération internationale en matière de cybercriminalité et de preuves électroniques, et pratiquement tous l'ont ratifiée. L'Irlande et la Suède sont toujours engagées dans le processus de ratification de la convention sur la cybercriminalité. La convention sur la cybercriminalité est un instrument international contraignant requérant des parties contractantes qu'elles définissent des infractions pénales spécifiques commises à l'encontre de réseaux électroniques ou au moyen desdits réseaux dans leur législation nationale et définissent également des pouvoirs et procédures spécifiques autorisant leurs autorités nationales à mener leurs enquêtes pénales, en ce compris en collectant des preuves électroniques. Elle encourage également la coopération internationale entre les parties contractantes. Il existe des mesures spécifiques visant à surmonter les difficultés posées par la volatilité des données. À cet égard, la convention prévoit la conservation rapide de données informatiques stockées. Étant donné que le transfert des preuves sécurisées à l'État requérant est subordonné à une décision finale sur la demande officielle d'entraide judiciaire, la conservation n'est pas soumise à l'ensemble des motifs de refus, en particulier la double incrimination n'est requise que dans des cas exceptionnels (article 29).

[17] Avis 2/2019 du CEPD sur le mandat de négociation d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontière aux preuves électroniques et avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un second protocole additionnel à la convention de Budapest sur la cybercriminalité.
[18] Disponible à l'adresse suivante: https://www.congress.gov/bill/115th-congress/house-bill/1625/text.
[19] https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_fr.
[20] https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.
[21] Exposé des motifs de la proposition de règlement, p. 2.
[22] Arrêt de la Cour de justice de l'Union européenne (ci-après la «CJUE») du 8 avril 2014, Digital Rights Ireland et Seitlinger, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 33, dans lequel la CJUE a jugé, à propos de l'établissement d'une limitation au droit au respect de la vie privée, qu'«*il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence*». Voir également l'arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, affaire C-207/16, ECLI:EU:C:2018:788, point 51.
[23] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 36, dans lequel la CJUE a jugé qu'une mesure «*est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la [c]harte puisqu'elle prévoit un traitement des données à caractère personnel*».
[24] Disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf. Voir la section II 4) du Guide du CEPD pour l'évaluation de la nécessité, p. 7 et l'avis 1/15 de la CJUE du 26 juillet 2017, ECLI:EU:C:2017:592, point 140: «*S'agissant du respect du principe de proportionnalité, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire [...]*».
[25] Les situations transfrontières désignent les situations dans lesquelles le fournisseur de services destinataire est établi ou représenté dans un autre État membre que l'autorité d'émission.
[26] Les situations nationales désignent les situations dans lesquelles le fournisseur de services destinataire est établi ou représenté dans le même État membre que l'autorité d'émission. Dans de tels cas, les autorités de cet État membre doivent recourir à des mesures nationales pour contraindre le fournisseur de services. Voir le considérant 15 de la proposition de règlement.
[27] Voir l'article 2, point 4, de la proposition de règlement pour la définition de l'expression «*proposer des services dans l'Union*». Il s'agit non seulement de permettre à des personnes dans un ou plusieurs État(s) membre(s) d'utiliser les services énumérés, mais aussi d'avoir un lien substantiel avec ce ou ces État(s) membre(s).
[28] Exposé des motifs de la proposition de directive, p. 3; voir également l'article 7 de la proposition de règlement. L'article 7, paragraphe 1, prévoit que l'injonction européenne de production et l'injonction européenne de conservation doivent être adressées directement au représentant légal désigné par le fournisseur de services concerné. L'article 7, paragraphe 2, prévoit comme option de repli que «*[s]i aucun représentant légal spécial n'a été désigné, l'injonction européenne de production et l'injonction européenne de conservation peuvent être adressées à tout établissement du fournisseur de services dans l'Union*».
[29] L'article 3 de la proposition de directive prévoit que les États membres veillent à ce que, qu'ils soient ou non établis dans l'Union, les fournisseurs de services proposant des services dans l'Union désignent au moins un représentant légal dans l'Union.
[30] En vertu de l'article 7 de la proposition de règlement, le destinataire des injonctions est en principe le représentant légal désigné par le fournisseur de services et, dans certains cas, l'établissement du fournisseur de services dans l'Union. Les termes «fournisseur de services» et «destinataire» sont utilisés dans le présent avis pour désigner le représentant légal ou l'établissement auquel l'injonction est transmise au moyen d'un certificat.
[31] Analyse d'impact, p. 94, 156 et 179.
[32] Les droits prévus à l'article 6 correspondent à ceux qui sont garantis par l'article 5 de la convention européenne des droits de l'homme et ont, conformément à l'article 52, paragraphe 3, de la charte, le même sens et la même portée. Voir les explications relatives à la charte des droits fondamentaux (2007/C 303/02).
[33] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, points 54 et 55.
[34] Voir le discours prononcé par M. Koen Lenaerts, président de la CJUE, à l'occasion d'une manifestation organisée en marge de la 40e Conférence internationale des commissaires à la protection des données et de la vie privée («The General Data Protection Regulation five months on», Le règlement général sur la protection des données cinq mois plus tard), disponible à l'adresse suivante: https://webcast.ec.europa.eu/the-general-data-protection-regulation-five-months-on-25-10-2018#.

[35] Exposé des motifs de la proposition de règlement, p. 16: «*Les données relatives aux transactions et celles relatives au contenu doivent faire l'objet d'exigences plus strictes pour refléter leur nature plus sensible et leur degré proportionnellement plus élevé d'intrusion par rapport aux deux catégories précédentes de données.*»
[36] Ces exigences sont énoncées aux articles 4, 5 et 6 de la proposition de règlement et concernent les infractions pénales pour lesquelles des injonctions de production ou de conservation de ces catégories de données peuvent être émises et l'autorité judiciaire qui émet ou valide l'injonction.
[37] En vertu de l'article 4, paragraphe 3, point a), de la proposition de règlement «vie privée et communications électroniques», on entend par «données de communications électroniques» «*le contenu de communications électroniques et les métadonnées de communications électroniques*».
[38] En vertu de l'article 4, paragraphe 3, point b), de la proposition de règlement «vie privée et communications électroniques», on entend par «contenu de communications électroniques» «*le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son*».
[39] En vertu de l'article 4, paragraphe 3, point c), de la proposition de règlement «vie privée et communications électroniques», on entend par «métadonnées de communications électroniques» «*les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication*».
[40] https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_fr.
[41] Exposé des motifs de la proposition de règlement, p. 2: «*La présente proposition vise à renforcer la sécurité juridique pour les autorités, les fournisseurs de services et les personnes concernées et à maintenir un niveau de qualité élevé pour les demandes des services répressifs, en garantissant la protection des droits fondamentaux, la transparence et l'obligation de rendre des comptes.*»
[42] Exposé des motifs de la proposition de règlement, p. 14.
[43] Analyse d'impact, p. 129: «*la définition des types de données (données relatives aux abonnés, au trafic et au contenu) varie considérablement d'un État membre à l'autre, alors que des catégories spécifiques de données existent dans plusieurs pays. Les données demandées aux fournisseurs de services sont généralement des données relatives aux abonnés (21 États membres) et au trafic (18 États membres), tandis que dans quelques États membres (neuf), il est également possible de demander des données relatives au contenu et d'«autres données» (quatre États membres).*»
[44] Voir l'avis 23/2018 du comité européen de la protection des données, p. 12: «*les quatre catégories proposées ne semblent pas clairement délimitées et la définition des «données relatives à l'accès» reste encore vague [...]*.»
[45] En vertu de l'article 18, paragraphe 3, de la convention sur la cybercriminalité, l'expression «données relatives aux abonnés» désigne «*toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service*».
[46] Voir le document de travail du comité de la convention cybercriminalité du Conseil de l'Europe intitulé «Conditions d'obtention des informations sur les abonnés concernant les adresses IP dynamiques par rapport aux adresses IP statiques: vue d'ensemble des décisions judiciaires et des développements pertinents», T-CY (2018)26 du 25 octobre 2018, qui examine la question de savoir si les adresses IP dynamiques devraient être soumises à des règles concernant l'obtention des informations sur les abonnés ou à des règles concernant l'obtention des données relatives au trafic (définies à l'article 1er, point d, de la convention) et qui conclut notamment que «*[l]'introduction de nouvelles catégories de données, comme les "données relatives à l'accès", pourrait conduire à de nouveaux malentendus au sujet des règles applicables à la conservation et à l'accès à ces données et compliquer leur application par les praticiens*».
[47] Voir les conclusions de l'avocat général du 3 mai 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:300, points 117 et 118:
«*il serait [...] souhaitable que la Cour s'abstienne de prendre position en faveur d'un quantum précis de peine encourue, car ce qui est adapté pour certains États membres ne le sera pas forcément pour d'autres et ce qui vaut à ce jour pour un type d'infractions ne vaudra pas nécessairement de façon irrévocable à l'avenir [...]*
[...] À ce dernier égard, je relève que, en l'espèce, la juridiction de renvoi fait état d'un risque d'inversion entre la règle générale et les dérogations prévues par la directive 2002/58, risque évoqué ci-dessus (132), lorsqu'elle indique que "le seuil de trois ans de prison [introduit en 2015 par le législateur espagnol (133)] concerne une

grande majorité des qualifications pénales". Autrement dit, d'après cette juridiction, la liste actuelle des infractions susceptibles de justifier, en Espagne, des restrictions aux droits protégés en vertu des articles 7 et 8 de la charte, qui a été instaurée par la réforme du code de procédure pénale, conduirait, en pratique, à ce que la majeure partie des infractions prévues au code pénal soient incluses dans ladite liste.»

[48] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 27.

[49] Arrêt de la CJUE du 21 décembre 2016, Tele2 Sverige et Watson e.a., affaires jointes C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 99.

[50] Arrêt de la CJUE du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 39 et arrêt de la CJUE du 21 décembre 2016, Tele2 Sverige et Watson e.a., affaires jointes C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 101.

[51] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, points 54 et 56.

[52] Voir les conclusions de l'avocat général du 3 mai 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:300, dans lesquelles il fournit des indications sur les critères qui permettraient de définir la notion d'«infractions graves» au sens de la jurisprudence de la CJUE, en particulier au regard du critère de la peine encourue.

[53] Analyse d'impact, p. 240

[54] Arrêt de la CJUE du 2 octobre 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788.

[55] Voir la section 3.1 du présent avis sur l'impérieuse nécessité de clarifier les catégories de données au titre de la proposition de règlement.

[56] Les données à caractère personnel doivent être traitées de façon à garantir une sécurité et une confidentialité appropriées, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées [principe d'intégrité et de confidentialité consacré à l'article 5, paragraphe 1, point f), du RGPD, et à l'article 4, paragraphe 1, point f), de la directive relative à la protection des données dans le domaine répressif]. La sécurité du traitement comprend notamment la capacité à garantir de manière constante la confidentialité et l'intégrité des systèmes de traitement.

[57] Le considérant 57 précise que «*les États membres doivent veiller [...] à ce que des politiques et mesures appropriées de protection des données s'appliquent à la transmission de données à caractère personnel par les autorités compétentes aux fournisseurs de services [...], y compris des mesures garantissant la sécurité des données Les fournisseurs de services doivent également offrir les mêmes garanties pour la transmission de données à caractère personnel aux autorités compétentes. Seules des personnes autorisées peuvent avoir accès aux informations contenant des données à caractère personnel pouvant être obtenues par des processus d'authentification. L'utilisation de mécanismes garantissant l'authenticité doit être envisagée, comme les systèmes nationaux d'identification électronique notifiés ou les services de confiance tels que prévus par le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE*».

[58] L'article 8, paragraphe 2, dispose uniquement que «*[l]'EPOC ou l'EPOC-PR sont transmis directement par tout moyen susceptible de produire une trace écrite dans des conditions permettant au destinataire d'établir son authenticité*» [soulignement ajouté].

[59] L'article 9 dispose que «*le destinataire veille à ce que les données requises soient transmises directement à l'autorité [...] comme indiqué dans l'EPOC*». La proposition de règlement ne fait mention d'aucune mesure de sécurité appropriée pour la transmission des données produites par les destinataires de l'EPOC. La proposition de règlement reste muette sur la sécurité des communications à la suite de la transmission d'un EPOC-PR.

[60] L'article 14, paragraphe 1, dispose uniquement que l'autorité d'émission peut transférer l'injonction accompagnée d'autres documents «*par tout moyen susceptible de garder une trace écrite dans des conditions permettant à l'autorité chargée de la mise en œuvre d'établir son authenticité*» [soulignement ajouté].

[61] Article 8 de l'orientation générale sur la proposition de règlement.

[62] Article 9 de l'orientation générale sur la proposition de règlement.

[63] Exposé des motifs de la proposition de règlement, p. 2.

[64] Voir l'analyse d'impact initiale «Inception Impact Assessment on Cross-border e-Justice in Europe (e-CODEX), disponible à l'adresse suivante: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3600084_en, p. 1: «*"e-CODEX" est un système informatique de coopération judiciaire transfrontière qui permet aux utilisateurs, qu'il s'agisse d'autorités judiciaires, de praticiens du droit ou de citoyens, d'envoyer et de recevoir en toute sécurité des documents, formulaires juridiques, éléments de preuve ou autres informations. Il fonctionne comme un réseau décentralisé de points d'accès, reliant entre eux les systèmes informatiques nationaux et européens. Un logiciel spécifique est nécessaire pour établir un point d'accès e-CODEX.*
Le système e-CODEX a été développé dans le cadre du marché unique numérique par un groupe d'États membres avec l'aide de subventions de l'Union. Plusieurs États membres utilisent déjà le système e-CODEX en appui aux

procédures juridiques transfrontières tant en matière civile que pénale, par exemple aux fins de l'échange de demandes d'entraide judiciaire entre ministères publics.»
Voir également le site internet d'e-CODEX, qui indique que le projet est arrivé à son terme, mais que *«[l]'objectif de Me-CODEX (Maintenance d'e-CODEX) est de faire le pont entre la fin du projet e-CODEX et la prise en charge de la maintenance d'e-CODEX par une agence européenne. Il faudra compter entre deux et quatre ans pour procéder à l'extension nécessaire du mandat de l'agence de l'Union. Étant donné que les États membres qui échangent des informations par l'intermédiaire d'e-CODEX n'abandonneront pas leurs solutions au terme du projet e-CODEX, une solution intermédiaire de maintenance doit être trouvée. La Commission européenne a exhorté le groupe permanent d'experts sur e-CODEX à fournir une solution pour assurer les opérations et élargir la communauté des utilisateurs. La solution, "Me-CODEX", fonctionnera sur la base d'un transfert harmonieux à une agence de l'Union, de la maintenance des modules e-CODEX, de l'extension à d'autres pays, de la gestion des parties prenantes/communautés et de la recherche et du développement. L'appui à d'autres procédures juridiques transfrontières que celles déjà soutenues par e-CODEX nécessitera la mise en place de projets différents. Ces projets peuvent bien sûr compter sur la gestion opérationnelle de Me-CODEX*» (https://www.e-codex.eu/sites/default/files/newsletter/newsletter_2016-6.html).

[65] Pour de plus amples informations sur SIRIUS, voir la réponse donnée par la Commission à la question écrite E-007204/2017: «*Compte tenu du nombre croissant de demandes d'appui opérationnel reçues des États membres, l'unité de l'Union européenne chargée du signalement des contenus sur l'internet (EU IRU) au sein d'Europol a récemment lancé SIRIUS afin de soutenir les enquêtes judiciaires en ligne. SIRIUS garantit un environnement sécurisé pour les informations relatives aux fournisseurs de services en ligne (FSL), en mettant à disposition des manuels, des conseils, des forums, des questions et des réponses, ainsi que des outils élaborés par les services répressifs en appui aux enquêtes en ligne. Il fournit, entre autres, des conseils aux enquêteurs sur le type de données qui peuvent être directement obtenues auprès de leurs services.*
Les informations fournies par SIRIUS ne comprennent aucune donnée à caractère personnel ni demande de suppression de compte utilisateur. SIRIUS est un outil de renforcement des capacités qui favorise l'échange de connaissances. Actuellement, 372 représentants des services répressifs des États membres de l'Union sont membres de SIRIUS et utilisent les lignes directrices sur 19 FSL ainsi que les 13 outils (fournis par l'unité EU IRU et les États membres de l'UE) pour soutenir les enquêtes en ligne.
L'unité EU IRU reste déterminée à signaler les contenus terroristes aux plateformes hôtes. À ce jour, l'unité EU IRU a évalué au total 42 066 éléments de contenu, qui ont abouti à 40 714 décisions de renvoi sur plus de 80 plateformes dans plus de 10 langues.»

[66] Exposé des motifs de la proposition de règlement, p. 19.

[67] Voir l'orientation générale 15292/18 du Conseil, note de bas de page 33, p. 36.

[68] Article 22 de la proposition de règlement et article 6 de la proposition de directive.

[69] Voir par exemple le règlement (UE) nº 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, JO L 351 du 20.12.2012, p. 1, en particulier les articles 75 et 81, qui prévoyaient que les obligations en matière de communication des informations devaient être remplies un an avant la date d'application des autres dispositions dudit règlement.
En vertu de l'article 4, point 12, du RGPD et de l'article 3, paragraphe 11, de la directive relative à la protection des données dans le domaine répressif, une violation de données à caractère personnel est définie comme «*une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données*».

[70] Voir l'article 11 de la proposition de règlement.

[71] Voir
http://www.ejtn.eu/Documents/About%20EJTN/Criminal%20Justice%202017/CJSWG%20meeting%20Brussels%2013-14%20March%202017/COMMON%20CONCLUSIONS%20EJTN%20Barcelona%20seminar.pdf

[72] Voir la liste de motifs d'objection mentionnés à l'article 14, ainsi que la jurisprudence de la CJUE dans le cadre du mandat d'arrêt européen (arrêt de la CJUE du 5 avril 2016, Pál Aranyosi et Robert Căldăraru c. Generalstaatsanwaltschaft Bremen, affaires jointes C-404/15 et C-659/15 PPU, ECLI:EU:C:2016:198, point 82 et suivants).

[73] Voir l'avis rendu le 14 février 2011 par l'Agence des droits fondamentaux sur le projet de directive concernant la décision d'enquête européenne, p. 10: «*D'une manière générale, le droit dérivé de l'Union doit respecter les normes en matière de droits fondamentaux. Voir l'arrêt de la CJUE du 9 novembre 2010, Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, affaires jointes C-92/09 et C-93/09, ECLI:EU:C:2010:662, dans lequel la CJUE a annulé des dispositions du droit dérivé de l'Union pour non-respect des droits fondamentaux.*»

[74] «*Voir l'article 70 du traité FUE.*»

[75] «*Le régime d'asile de l'Union, dans lequel le droit primaire établit le principe selon lequel les États membres de l'Union doivent se considérer mutuellement comme "constituant des pays d'origine sûrs", permet toujours de*

déroger à cette présomption afin de garantir que les droits fondamentaux d'une personne puissent être pris en considération dans des cas exceptionnels. Voir l'article unique, point d), du protocole 24 des traités».

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

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

[78] Le considérant 35 *quater* de l'orientation générale du Conseil semble justifier cette limitation par le raisonnement suivant: «*À l'inverse des données non relatives au contenu, les données relatives au contenu sont particulièrement sensibles parce que les personnes peuvent y révéler des opinions ou des détails sensibles concernant leur vie privée, ce qui justifie un traitement différent et l'intervention des autorités de l'État chargé de la mise en œuvre à un stade précoce de la procédure.*» À cet égard, le CEPD tient à rappeler que, comme il l'a indiqué dans sa plaidoirie lors de l'audience conjointe dans l'affaire C-623/17 (Privacy International), les affaires jointes C-511/18 et C-512/18 (La Quadrature du Net e.a.) et l'affaire C-520/18 (Ordre des barreaux francophones et germanophone e.a.), «*[l]es autres données relatives aux communications électroniques – lesdites "métadonnées" [...] peuvent être aussi révélatrices que le contenu réel des communications*». «*Nous devons également garder à l'esprit que la distinction entre "contenu" et "métadonnées" n'est pas aussi nette dans un environnement de services multiples comme l'internet. C'est la raison pour laquelle, dans le contexte de la proposition de règlement "vie privée et communications électroniques", le CEPD a conseillé d'attribuer un niveau élevé de protection aux métadonnées, ainsi qu'aux données relatives au contenu*», voir la note de plaidoirie du CEPD (p. 4 et 5), disponible sur son site web https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-cases-c-62317_en

[79] Analyse d'impact, p. 14: «*Les demandes de données non relatives au contenu sont plus nombreuses que celles de données relatives au contenu, tant à l'intérieur qu'à l'extérieur de l'Union. Les données non relatives au contenu provenant de communications électroniques sont le plus souvent demandées.*»

[80] Voir l'article 7 *bis*.

[81] Voir la note de bas de page 34, p. 37 de l'orientation générale du Conseil sur la proposition de règlement: «*La République tchèque, la Finlande, l'Allemagne, la Grèce, la Hongrie et la Lettonie ont émis une réserve sur la procédure de notification, préconisant qu'elle ait davantage d'effets et couvre aussi les données relatives aux transactions et la clause relative aux droits fondamentaux, autrement dit, qu'elle donne à l'autorité notifiée des motifs de refus. Par ailleurs, une logique inverse devrait être retenue pour déterminer ce qu'est un "cas national". Enfin, l'Allemagne préconise que l'injonction soit soumise et non le certificat, tandis que la République tchèque estime qu'il faudrait soumettre les deux.*»

[82] La question a également été soulevée par le juge de la Cour européenne des droits de l'homme (CEDH), le professeur Dr Bošnjak, à titre personnel, lors de l'audition sur les preuves électroniques organisée par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) du Parlement européen le 27 novembre 2018 (en particulier le passage 16.55-16.58, qui porte précisément sur ce point – «*En ce qui concerne le droit de l'État chargé de la mise en œuvre, il semble qu'il ne soit d'aucune pertinence selon la proposition existante. Du point de vue de la convention, cela peut poser un problème parce que les hautes parties contractantes à la CEDH, y compris les 28 États membres de l'Union, sont responsables de la protection des droits de l'homme sur le territoire sous sa juridiction. [...] Ils doivent mettre en place un cadre réglementaire et garantir une protection juridique, voire judiciaire, dans des cas particuliers. [...] Lorsque les autorités de l'État chargé de la mise en œuvre sont amenées à traiter un grief dans le cadre duquel l'on se trouve en présence d'une insuffisance manifeste de protection d'un droit garanti par la convention et que le droit de l'Union européenne ne permet pas de remédier à cette insuffisance, elles ne peuvent renoncer à examiner ce grief au seul motif qu'elles appliquent le droit de l'Union. C'est ce qui ressort clairement de l'arrêt Avotiņš c. Lettonie et qui a été confirmé à plusieurs reprises par la suite. La proposition, telle qu'elle vous est présentée, crée une situation plutôt unique du point de vue de la jurisprudence de la CEDH. L'intervention prévue à l'article 8 aurait lieu sans la participation des autorités de l'État chargé de la mise en œuvre. Il y a lieu de se demander si cela est conforme à la CEDH. Il pourrait y avoir une attente légitime que le droit de l'État chargé de la mise en œuvre s'applique dans chaque situation particulière. Cela affecterait l'appréciation de la légalité [...]*»). Voir: http://www.europarl.europa.eu/ep-live/en/committees/video?event=20181127-1430-COMMITTEELIBE.

[83] À l'exception des infractions définies au niveau de l'Union, énumérées à l'article 5, paragraphe 4, point b), de la proposition de règlement.

[84] Avis 23/2018 du comité européen de la protection des données, section 2, point b).

[85] Voir également l'exposé du juge de la CEDH, le professeur Dr Bošnjak, à titre personnel, lors de l'audition sur les preuves électroniques organisée par la commission LIBE du Parlement européen le 27 novembre 2018 (note de bas de page 82 ci-dessus).

[86] Voir la section 3.2 du présent avis.

[87] Voir l'avis 2/2019 du CEPD, paragraphe 28, et l'avis 3/2019 du CEPD, paragraphe 53.

[88] Analyse d'impact, p. 37.

[89] Considérant 36.

[90] Considérant 19 de la proposition de règlement: «*Le présent règlement régule la collecte des données stockées uniquement, c'est-à-dire des données détenues par un fournisseur de services au moment de la réception d'un certificat d'injonction européenne de production ou de conservation. Il ne prévoit pas d'obligation générale de conservation des données, et n'autorise pas l'interception de données ou l'obtention de données stockées à un moment ultérieur à la réception d'un certificat d'injonction de production ou de conservation*.»

[91] Article 5, paragraphe 1, point e), du RGPD et article 4, paragraphe 1, point e), de la directive relative à la protection des données dans le domaine répressif.

[92] C'est le cas lorsque les données sont conservées si le fournisseur de services qui a reçu un EPOC ne les produit pas immédiatement.

[93] Avis 23/2018, section 7, point d), du comité européen de la protection des données: «Les injonctions européennes de conservation ne seront pas utilisées pour contourner les obligations de conservation de données qui incombent aux fournisseurs de services».

[94] Voir la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM(2017) 10 final (ci-après la «proposition de règlement "vie privée et communications électroniques"»).

[95] Article 12 *bis*, paragraphe 3.

[96] Par exemple, Facebook, Google, Microsoft, Twitter et Apple; voir l'analyse d'impact, p. 14.

[97] Par exemple, une disposition similaire figure à l'article 8 de la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne [COM(2018) 640 final].

[98] L'article 5 fixe les conditions d'émission d'une injonction européenne de production. Le libellé de la disposition manque toutefois de clarté. L'article 5, paragraphe 7, dispose que «*[s]i l'autorité d'émission a des raisons de croire que les données requises relatives aux transactions ou au contenu sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre du fournisseur de services destinataire [...], l'autorité d'émission doit demander des éclaircissements avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État membre concerné, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen*». En outre, «*[s]i l'autorité d'émission constate que les données requises relatives à l'accès, aux transactions ou au contenu sont protégées par ces immunités et privilèges [...], elle n'émet pas l'injonction européenne de production*» [soulignement ajouté].

[99] Voir l'article 5, paragraphe 7, de l'orientation générale du Conseil.

[100] Il semble que ce motif d'objection soit également disponible pour l'injonction européenne de conservation.

[101] Voir l'exposé des motifs de la proposition de règlement, p. 21: «*[...] si la procédure de mise en œuvre est tout de même lancée, le destinataire peut lui-même s'opposer à l'injonction devant l'autorité chargée de la mise en œuvre. Il peut y procéder sur la base des motifs avancés, à l'exception des immunités et privilèges*.»

[102] Voir l'article 7 *bis* de l'orientation générale du Conseil. La disposition ne prévoit qu'une possibilité pour l'autorité compétente de l'État chargé de la mise en œuvre d'informer l'autorité d'émission (et non une obligation).

[103] L'article 18 dispose que *«la juridiction de l'État d'émission garantit que, pendant la procédure pénale pour laquelle l'injonction a été émise, ces motifs sont pris en considération de la même manière que s'ils avaient été prévus par sa législation nationale lors de l'évaluation de la pertinence et de la recevabilité des preuves concernées. La juridiction peut consulter les autorités de l'État membre pertinent, le Réseau judiciaire européen en matière pénale ou Eurojust*».

[104] Dans l'orientation générale du Conseil, elle a été limitée aux situations dans lesquelles la personne concernée ne réside pas dans l'État d'émission (article 12 *bis*).

[105] L'orientation générale du Conseil ne prévoit que la possibilité, et non l'obligation, pour l'autorité d'émission de demander aux autorités de l'État chargé de la mise en œuvre d'exercer leur pouvoir de lever le privilège ou l'immunité (article 5, paragraphe 8).

[106] Un tel motif existe en vertu de l'article 11 de la directive DEE.

[107] Avis 23/2018 du comité européen de la protection des données, section 5, point b) Représentant légal, p. 11.

[108] L'exposé des motifs de la proposition de directive énonce ce qui suit (p. 3): «*L'obligation de désigner un représentant légal pour les prestataires qui ne sont pas établis dans l'UE, mais qui offrent des services au sein de celle-ci est déjà énoncée dans certains actes du droit de l'Union applicables dans des domaines particuliers. Tel est le cas, par exemple, du règlement général sur la protection des données [règlement (UE) 2016/679] (article 27) et de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (article 18). La proposition de la Commission relative à un règlement «vie privée et communications électroniques» contient également une telle obligation (article 3).*» L'exposé des motifs (p. 5) indique également que les représentants légaux désignés en vertu de la directive proposée peuvent cumuler d'autres fonctions, dont celles de représentants en vertu du RGPD et de la proposition de règlement «vie privée et communications électroniques». En outre, le considérant 6 de la proposition de directive fait référence au RGPD et à l'obligation qui y est faite de désigner un représentant légal

dans l'Union sous certaines conditions. De même, l'analyse d'impact (p. 91) indique que le représentant légal désigné en vertu de la proposition de directive «*pourrait couvrir plusieurs fonctions (représentants désignés en vertu du RGPD, du règlement "vie privée et communications électroniques" et d'une injonction européenne de production), ce qui permettrait de réduire les coûts*» pour les fournisseurs de services.

[109] À cet égard, le groupe de travail «Article 29» a souligné dans sa déclaration concernant la protection des données et les aspects relatifs au respect de la vie privée de l'accès transfrontalier aux preuves électroniques que «*[s]i le représentant légal désigné en vertu du RGPD est censé être le point de contact des autorités de contrôle des responsables du traitement ou des sous-traitants pour l'exécution de leurs obligations, le représentant désigné en vertu de la mesure envisagée a pour mission de faire exécuter l'injonction de production émise par l'autorité compétente*».

[110] En vertu de la proposition de directive, l'obligation de désigner un représentant légal est imposée à tous les fournisseurs de services qui proposent des services dans l'Union au sens de la proposition (article 2, point 3, lu en liaison avec le considérant 13), qu'ils soient ou non établis dans l'Union.

En vertu du RGPD (article 3, paragraphe 2, lu en liaison avec l'article 27), l'obligation de désigner un représentant est imposée aux responsables du traitement ou aux sous-traitants qui ne sont pas établis dans l'Union, mais qui traitent des «*données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union*», et les activités de traitement sont liées à l'offre de biens ou de services ou au «*suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein l'Union*» [soulignement ajouté]. En outre, l'article 27, paragraphe 2, du RGPD dispose que cette obligation ne s'applique pas «*à un traitement qui est occasionnel, qui n'implique pas un traitement à grande échelle des catégories particulières de données visées à l'article 9, paragraphe 1, ou un traitement de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10, et qui n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement; ou à une autorité publique ou à un organisme public*».

[111] L'article 9 fixe des délais pour répondre aux EPOC. Les données requises doivent être transmises «*au plus tard 10 jours après la réception de l'EPOC, sauf si l'autorité d'émission indique les raisons d'une divulgation anticipée*». En outre, la proposition de règlement prévoit que «*[d]ans les cas d'urgence, le destinataire transmet les données requises sans retard injustifié au plus tard [six] heures après la réception de l'EPOC*». En ce qui concerne l'EPOC-PR, le destinataire conserve les données ou prend contact avec l'autorité d'émission si le certificat ne peut être exécuté, sans retard injustifié dès réception du certificat (article 9, paragraphe 2). Les «cas d'urgence» sont définis à l'article 2, point 15, comme «*les situations où il existe une menace imminente pour la vie ou l'intégrité physique d'une personne ou pour une infrastructure critique telle que définie à l'article 2, point a), de la directive 2008/114/CE du Conseil*».

[112] Article 12, paragraphe 3, de la directive DEE.

[113] Article 12, paragraphe 4, de la directive DEE.

[114] L'article 13 de la proposition de règlement impose aux États membres de prévoir dans leur législation nationale des sanctions pécuniaires qui sont «*effectives, proportionnées et dissuasives*» en cas de non-respect d'une injonction. En cas de non-respect d'une injonction, l'article 14, paragraphe 3, prévoit que l'autorité chargée de la mise en œuvre informe le destinataire de la possibilité de soulever les objections énumérées à l'article 14, paragraphes 4 et 5, et rappelle également les sanctions applicables en cas de non-conformité.

[115] En tout état de cause, de telles sanctions ne devraient pas être imposées aux destinataires qui s'opposent à une injonction parce qu'ils estiment de bonne foi qu'elle viole la charte de l'Union européenne.

[116] Elle couvre «tout service qui permet à ses utilisateurs d'envoyer ou de recevoir des communications filaires ou électroniques ou par fil» [Titre 18 du code des États-Unis, article 2510, paragraphe 15)].

[117] Voir le nouveau point (i) tel qu'il est inséré au chapitre 119 «Interception des communications filaires et électroniques et interception des communications orales» du titre 18 du code des États-Unis par le CLOUD Act.

[118] Articles 15 et 16 de la proposition de règlement. Exposé des motifs de la proposition de règlement, p. 21: «*En fixant des normes strictes, elles aspirent à encourager les pays tiers à mettre en place un niveau de protection similaire. Dans la situation inverse, lorsque les autorités d'un pays tiers cherchent à obtenir les données d'un citoyen européen auprès d'un fournisseur de services de l'UE, la législation de l'Union ou des États membres relative à la protection des droits fondamentaux, comme l'acquis en matière de protection des données, permettent d'empêcher de la même façon la divulgation de ces données. L'Union européenne attend des pays tiers qu'ils respectent ces interdictions tout comme le fait la présente proposition.*»

[119] Documents 9114/19 et 9116/19 du Conseil, disponibles à l'adresse suivante: https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[120] Addendum à la décision, point I.1, document du Conseil 9666/19.

[121] Addendum à la décision, point II.1. a), document 9664/19 du Conseil.

[122] En vertu de cette disposition, «[l]e présent règlement ne porte pas atteinte aux autres instruments, accords et arrangement de l'UE et au niveau international relatifs à [...] la collecte de preuves qui relèveraient également du champ d'application du présent règlement».