Avis 23/2018 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]

Adopté le 26 septembre 2018

Table des matières

Le Comité européen de la protection des données (CEPD)

considérant l'article 70, paragraphe 1, point b), du 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,

A ADOPTÉ L'AVIS SUIVANT:

Introduction

En avril 2018, la Commission a présenté une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et une proposition de directive établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale. Les deux propositions COM(2018) 225 final et COM(2018) 226 final sont complémentaires. L'objectif général poursuivi par la Commission est d'améliorer la coopération entre les autorités des États membres et les fournisseurs de services, notamment ceux établis dans des pays tiers, et de proposer des solutions au problème que posent la détermination de la compétence et l'exécution des décisions dans le cyberespace.

Tandis que le projet de règlement prévoit les règles et les procédures relatives à l'émission, à la signification et à l'exécution des injonctions de production et de conservation aux fournisseurs de services de communications électroniques, le projet de directive établit, elle, les règles minimales applicables à la désignation d'un représentant légal pour des fournisseurs de services qui ne sont pas établis dans l'UE.

En novembre 2017[1], avant que la Commission ne présente de projets de textes, le groupe de travail « Article 29 » a rappelé la nécessité de garantir que toute proposition législative se conforme pleinement à l'acquis de l'UE existant en matière de protection des données, ainsi qu'au droit de l'UE et à la jurisprudence en général.

En particulier, le groupe de travail « Article 29 » a mis en garde contre les limitations des droits à la protection des données et à la vie privée en ce qui concerne les données traitées par les fournisseurs de télécommunications et de la société de l'information, en particulier lorsqu'elles sont traitées ultérieurement par les autorités répressives, a rappelé la nécessité d'assurer la cohérence de tout instrument européen avec la convention existante de Budapest sur la cybercriminalité du Conseil de l'Europe et avec la directive européenne sur la décision d'enquête européenne, et a recommandé de clarifier les règles de procédure respectives régissant l'accès aux preuves électroniques aux niveaux national et de l'Union afin de garantir que le nouvel instrument ne confère pas aux autorités de nouveaux pouvoirs dont elles ne disposeraient pas au niveau national. Outre ces observations générales, le groupe de travail « Article 29 » s'est exprimé sur les options législatives envisagées à l'époque par la Commission concernant les catégories de données concernées et les garanties correspondantes relatives à l'accès à celles-ci, sur la possibilité d'émettre des injonctions/demandes de production pour contraindre les fournisseurs de services à fournir des données situées en dehors

[1] Voir la déclaration du groupe de travail « Article 29 » (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

de l'UE, et sur les conditions de fond et de procédure nécessaires pour garantir un accès direct aux données.

Les propositions concrètes sur les preuves électroniques étant désormais disponibles, le Comité européen de la protection des données souhaite présenter une analyse plus détaillée des instruments juridiques proposés sous l'angle de la protection des données.

1. Base juridique de la proposition de règlement (article 82 TFUE)

La base juridique suggérée pour le projet de règlement relatif aux preuves électroniques est l'article 82, paragraphe 1, TFUE concernant la coopération judiciaire en matière pénale, qui dispose :

> «1. La coopération judiciaire en matière pénale dans l'Union est fondée sur le principe de reconnaissance mutuelle des jugements et décisions judiciaires et inclut le rapprochement des dispositions législatives et réglementaires des États membres dans les domaines visés au paragraphe 2 et à l'article 83.
>
> Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, adoptent les mesures visant:
>
> a) à établir des règles et des procédures pour assurer la reconnaissance, dans l'ensemble de l'Union, de toutes les formes de jugements et de décisions judiciaires;
>
> b) à prévenir et à résoudre les conflits de compétence entre les États membres;
>
> c) à soutenir la formation des magistrats et des personnels de justice;
>
> d) à faciliter la coopération entre les autorités judiciaires ou équivalentes des États membres dans le cadre des poursuites pénales et de l'exécution des décisions.»

Comme le souligne la Commission dans l'analyse d'impact accompagnant les propositions, «l'article 82, paragraphe 1, précise que la coopération judiciaire en matière pénale est fondée sur le principe de reconnaissance mutuelle. Cette base juridique couvrirait une éventuelle législation sur la coopération directe avec les fournisseurs de services, dans laquelle l'autorité de l'État membre d'émission s'adresserait directement à une entité (le fournisseur de services) de l'État d'exécution et imposerait même des obligations à celle-ci. Cela introduirait une nouvelle dimension dans la reconnaissance mutuelle, qui va au-delà de la coopération judiciaire traditionnelle dans l'Union, fondée jusqu'à présent sur des procédures impliquant deux autorités judiciaires, l'une dans l'État d'émission et l'autre dans l'État d'exécution.» (soulignement ajouté)

Compte tenu de l'utilisation nouvelle de cette base juridique dans le cadre des demandes directes entre les autorités publiques et les parties privées, le CEPD regrette que la Commission n'ait produit aucune analyse ou évaluation complémentaire.

En effet, comme l'a déjà souligné le groupe de travail dans sa déclaration précédente, le CEPD continue de rappeler ses doutes quant au caractère approprié de cette base juridique, qui sont corroborés par l'analyse de la Cour de justice de l'Union européenne (CJUE) et son avocat général dans l'avis 1/15. Parmi les développements concernant la validité de l'article 82 en tant que base juridique du projet d'accord PNR (accord sur les données des dossiers passagers) entre l'UE et le Canada, la Cour a souligné que l'autorité compétente canadienne «*ne constitue ni une autorité judiciaire ni une autorité équivalente*»[2]. Dans le contexte des propositions relatives aux preuves électroniques, l'un des objectifs

[2] Voir le point 103 de l'avis 1/15 et le point 108 des conclusions de l'avocat général dans cette affaire.

principaux poursuivis semble être, comme l'affirme la Commission, d'éviter une coopération judiciaire «trop fastidieuse». Par conséquent, la proposition est fondée sur le principe selon lequel la coopération doit avoir lieu entre une autorité et un fournisseur de services plutôt qu'entre deux autorités. La procédure prévue place donc au premier chef des entités privées comme la partie destinataire et les met en position de répondre à des demandes émanant d'autorités judiciaires.

Le CEPD relève que le processus d'exécution d'injonctions de production ou de conservation pourrait nécessiter l'intervention d'une autorité destinataire dans le cas où le fournisseur de services destinataire ne s'acquitterait pas de ses obligations ce qui déclenchera ainsi la nécessité de demander une exécution a posteriori de l'injonction. Toutefois, l'objectif principal de la procédure mise en place étant précisément de ne pas faire intervenir une autorité destinataire, le CEPD doute que cette procédure subsidiaire puisse justifier l'utilisation de l'article 82 comme seule base juridique de l'instrument.

Par conséquent, le CEPD considère que, pour que l'article 82 puisse servir de base juridique, les principales étapes procédurales de la coopération doivent avoir lieu entre deux autorités judiciaires et qu'une autre base juridique devrait être utilisée pour ce type de coopération.

2. Nécessité des propositions en matière de preuves électroniques par rapport aux traités d'entraide judiciaire et à la décision d'enquête européenne

Le CEPD observe que le Commission s'engage à examiner les obstacles aux enquêtes en matière pénale, en particulier en ce qui concerne la question de l'accès aux preuves électroniques. Dans son exposé des motifs, la Commission présente le contexte de la proposition et souligne la nature volatile des preuves électroniques, leur dimension internationale ainsi que la nécessité d'adapter les mécanismes de coopération à l'ère numérique. Les propositions de règlement et de directive relatifs au transfert de preuves électroniques et à l'accès à ces preuves ne visent pas à remplacer les instruments de coopération antérieurs en matière pénale tels que la Convention de Budapest, les accords d'entraide judiciaire et la décision d'enquête européenne (directive concernant la décision d'enquête européenne en matière pénale). Selon la Commission, les propositions relatives aux preuves électroniques visent à améliorer la coopération judiciaire en matière pénale entre les autorités et les fournisseurs de services au sein de l'Union européenne ainsi qu'avec les pays tiers, en particulier les États-Unis d'Amérique.

Étant donné que ces nouveaux instruments supplémentaires seront spécifiquement consacrés à l'accès aux preuves électroniques et au transfert de preuves électroniques, le CEPD va évaluer la valeur ajoutée apportée par ces instruments par rapport à la directive concernant la décision d'enquête européenne et aux accords d'entraide judiciaire.

a) La nécessité des propositions en matière de preuves électroniques en comparaison des garanties fournies par la décision d'enquête européenne et les accords d'entraide judiciaire

Le principal argument avancé par la Commission en faveur des propositions relatives aux preuves électroniques est d'accélérer le processus pour recueillir et obtenir des preuves électroniques qui sont stockées et/ou détenues par des fournisseurs de services établis dans une autre juridiction.

Le CEPD déplore cependant que la nécessité de disposer d'un nouvel instrument pour organiser l'accès aux preuves électroniques n'ait pas été démontrée dans l'analyse d'impact. En effet, dans les propositions manque la démonstration qu'aucun autre moyen moins intrusif n'aurait pu être utilisé pour atteindre l'objectif poursuivi par la proposition relative aux preuves électroniques, alors que d'autres solutions auraient pu être envisagées. Par exemple, la possibilité de modifier et d'améliorer la directive concernant la décision d'enquête européenne en matière pénale aurait pu être examinée et aurait également répondu à l'exigence spécifique, établie dans ladite directive, d'évaluer la nécessité de modifier le texte avant le 21 mai 2019[3]. Une autre possibilité aurait pu consister à prévoir l'utilisation d'injonctions de conservation pour geler les données en attendant la présentation d'une demande officielle fondée sur un accord d'entraide judiciaire. Ces options auraient permis de maintenir les garanties prévues dans ces instruments tout en assurant que les données à caractère personnel recherchées ne sont pas effacées.

Le CEPD observe que les délais établis dans la directive concernant la décision d'enquête européenne en matière pénale sont plus longs que ceux prévus dans la proposition relative aux preuves électroniques. En effet, l'autorité d'exécution dispose de 30 jours pour prendre sa décision relative à la reconnaissance de la demande[4] et doit ensuite exécuter l'injonction dans les 90 jours[5]. Le CEPD considère que l'octroi de 30 jours de réflexion aux autorités d'exécution au titre de la décision d'enquête européenne en matière pénale constitue une garantie cruciale leur permettant d'évaluer si la demande d'exécution est fondée et si elle respecte toutes les conditions d'émission et de transmission d'une décision d'enquête européenne[6].

Le CEPD est préoccupé par le fait que le délai de 10 jours prévu dans les propositions relatives aux preuves électroniques pour l'exécution du certificat d'injonction européenne de production (EPOC), sans aucun délai de réflexion, empêche d'évaluer correctement si l'EPOC remplit tous les critères et s'il y est correctement répondu.

Par conséquent, le CEPD recommande qu'un délai plus long soit accordé au destinataire de l'EPOC pour déterminer si l'injonction doit ou non être exécutée.

Le CEPD observe que, dans le cas d'une injonction européenne de conservation (EPOC-PR), rien ne garantit que la conservation des données sera limitée à la période nécessaire pour produire les données. En effet, la durée de conservation des données pourrait dépasser 60 jours dans la mesure où aucun délai n'est fixé pour que l'autorité émettrice de l'injonction informe le destinataire qu'il ne doit pas transmettre les données ou pour qu'elle retire une injonction de production. Par conséquent, le CEPD recommande au moins qu'un délai soit accordé à l'autorité émettrice pour ne pas émettre ou retirer l'injonction de production afin de respecter le principe de minimisation des données établi dans le RGPD[7].

Enfin, le CEPD relève que la directive concernant la décision d'enquête européenne en matière pénale établit le renvoi par l'État d'émission d'éléments de preuve à l'autorité d'exécution[8]. Toutefois, le règlement relatif aux preuves électroniques reste silencieux quant à cette possibilité. Ce qu'il advient des preuves électroniques après leur transmission à l'autorité émettrice reste obscur.

[3] Voir l'article 37 de la directive concernant la décision d'enquête européenne en matière pénale.
[4] Article 12, paragraphe 3, de la directive concernant la décision d'enquête européenne en matière pénale
[5] Article 12, paragraphe 4, de la directive concernant la décision d'enquête européenne en matière pénale
[6] Article 6 de la directive concernant la décision d'enquête européenne en matière pénale
[7] Article 5, paragraphe 1, point c), du RGPD.
[8] Article 13, paragraphes 3 et 4, de la directive concernant la décision d'enquête européenne en matière pénale

Par conséquent, le CEPD recommande que la proposition de règlement fournisse davantage d'informations sur l'utilisation des preuves électroniques après leur transfert à l'autorité émettrice afin de respecter le RGPD et le principe de transparence[9] ainsi que le principe de spécificité établi par les traités d'entraide judiciaire.

b) L'abandon du principe de double incrimination

Le CEPD reconnaît que la reconnaissance mutuelle dépend de l'application du principe de double incrimination, qui est un moyen pour les États membres de préserver leur souveraineté. Toutefois, la double incrimination est de plus en plus perçue comme un obstacle au déroulement fluide de la coopération judiciaire. Les États membres de l'UE sont de plus en plus enclins à coopérer même si les mesures d'enquête concernent des actes qui ne sont pas considérés comme des infractions dans leur droit national. Le CEPD rappelle toutefois que le principe de double incrimination vise à fournir une garantie supplémentaire pour 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. Ce principe empêcherait par exemple un État d'exiger l'aide d'un autre État pour emprisonner une personne en raison de ses opinions politiques si ces dernières ne sont pas incriminées dans l'État auquel la demande est adressée ou de poursuivre une personne ayant subi un avortement si celle-ci réside dans un autre État où l'avortement n'est pas illégal. Le principe de double incrimination s'accompagne aussi souvent de limitations ou de garanties supplémentaires concernant les sanctions si celles-ci diffèrent trop entre l'État demandeur et l'État d'exécution. L'exemple le plus flagrant est l'engagement à ne pas appliquer la peine de mort dans certains traités d'entraide judiciaire lorsqu'elle n'existe pas dans la législation de l'une des deux parties.

Le CEPD observe que le principe de la double incrimination ne figure pas dans la proposition de règlement relatif aux preuves électroniques. Toutefois, cette exclusion n'entraîne pas seulement la suppression des formalités habituelles de reconnaissance mutuelle, mais aussi la suppression des garanties liées au principe même de la double incrimination.

En effet, le CEPD souligne qu'aucune référence n'est faite à la législation du pays dans lequel le fournisseur de services destinataire de la demande est établi et que la conservation de toutes données, ainsi que la production de données relatives aux abonnés et des données relatives à l'accès peuvent être demandées pour toutes les infractions pénales[10], qu'il existe ou non des infractions pénales similaires dans d'autres États membres.

Dans l'intervalle, les injonctions de production ne peuvent être émises et exécutées que s'il existe une mesure similaire pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission[11]. De plus, comme expliqué par la Commission dans l'exposé des motifs de la proposition de règlement, la spécificité des données relatives aux transactions et au contenu est établie, car ces données sont considérées comme plus sensibles. En effet, les injonctions portant sur des données relatives aux transactions ou au contenu sont basées sur un seuil constitué par une peine privative de liberté maximale d'au moins trois ans visant à garantir le respect du principe de proportionnalité et des droits des personnes concernées[12]. Toutefois, le CEPD souligne qu'il n'existe, au sein de l'UE,

[9] Article 5, paragraphe 1, point a), du RGPD.
[10] Article 5, paragraphe 3, et article 6, paragraphe 2, de la proposition de règlement relatif aux preuves électroniques.
[11] Article 5, paragraphe 2, de la proposition de règlement relatif aux preuves électroniques.
[12] Article 5, paragraphe 4, point a), de la proposition de règlement relatif aux preuves électroniques.

aucune harmonisation quant aux infractions pénales punies par une peine privative de liberté d'une durée maximale d'au moins trois ans.

Le CEPD s'oppose à l'abandon du principe de double incrimination, qui vise à garantir qu'un État ne peut pas compter sur l'aide d'autres États pour faire appliquer son droit pénal national en dehors de son territoire par un État qui ne partage pas la même approche, compte tenu en particulier de la disparition d'autres garanties traditionnelles importantes en matière de droit pénal [voir ci-dessous le point 3 concernant les critères de localisation et le point 7 g) concernant des conflits potentiels avec les législations de pays tiers].

c) La conséquence de s'adresser directement aux entreprises

Le CEPD reconnaît que les preuves électroniques sont de plus en plus disponibles depuis des infrastructures privées qui peuvent se trouver en dehors du pays d'enquête appartenant à des fournisseurs de services.

Le CEPD observe qu'à la suite des décisions *Yahoo!*[13] et *Skype*[14] rendues en Belgique et dans le contexte des attentats terroristes, une coopération plus fluide et plus rapide entre les entités publiques et privées s'avère nécessaire. Dans l'analyse d'impact, la Commission fait référence à trois types d'instruments de procédure impliquant à la fois les autorités publiques et les fournisseurs de services. Il s'agit de la coopération judiciaire, de la coopération directe et de l'accès direct. Si la première n'impose pas la responsabilité de l'exécution de la décision d'enquête européenne au fournisseur de services mais à l'autorité d'exécution[15], la seconde, la coopération directe, est fondée sur la coopération du fournisseur de services. L'instrument le plus intrusif est l'accès direct auprès d'un fournisseur de services puisque les autorités publiques sont en mesure d'accéder aux données sans l'aide d'un intermédiaire.

Par conséquent, le CEPD craint que, lorsque la demande leur est adressée directement, les fournisseurs de services n'assurent pas la protection des données à caractère personnel aussi efficacement que les autorités publiques peuvent et doivent le faire et souligne que cela entraîne également l'inapplicabilité de certaines garanties de procédure prévues dans le cadre de la coopération judiciaire pour les particuliers, ainsi que pour les entreprises elles-mêmes[16]. En effet, par exemple, un fournisseur de services qui reçoit une demande devrait saisir le tribunal d'un autre État (membre) pour contester l'injonction, alors que, dans le cadre de la coopération judiciaire, il serait confronté à ses propres autorités. Le CEPD recommande l'inclusion, dans la proposition de règlement, de motifs supplémentaires pour certifier que les fournisseurs de services protégeront les droits fondamentaux individuels tels que la protection des données à caractère personnel et le respect de la vie privée et familiale, ainsi que l'information de l'autorité compétente en matière de protection des données afin de garantir qu'un contrôle est possible.

[13] Cour de cassation de Belgique, YAHOO! Inc., N° P.13.2082.N du 1er décembre 2015.
[14] Tribunal correctionnel d'Anvers, division Malines de Belgique, Nº ME20.F1.105151-12 du 27 octobre 2016. (Skype a fait appel de la décision).
[15] Articles 10 à 16
[16] Voir également, du point de vue de la protection des données internationales, le document «Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes», Groupe de travail international sur la protection des données dans les télécommunications, 63e réunion, 9 et 10 avril 2018, Budapest (Hongrie).

3. Le nouveau chef de compétence et ladite «disparition du critère de localisation»

Le CEPD relève que la Commission souligne que l'un des principaux changements apportés par ces propositions est la disparition du critère de localisation et la possibilité pour les autorités compétentes de demander la conservation et la production de données quel que soit l'endroit où ces données sont effectivement stockées.

Du point de vue de la protection des données, le fait que la législation de l'UE en matière de protection des données s'applique quel que soit l'endroit où les données des personnes concernées sont stockées n'a rien de nouveau. En effet, l'applicabilité du RGPD dépend soit du fait que le responsable du traitement ou le sous-traitant est établi dans l'UE, soit du fait que les données des personnes concernées de l'UE sont traitées même lorsque le responsable du traitement ou le sous-traitant n'est pas établi sur le territoire de l'UE[17], auquel cas ces-derniers doivent également désigner un représentant légal dans l'UE[18]. Du point de vue de la protection des données, il est important d'observer que la portée territoriale étendue vise à offrir une protection plus complète aux personnes concernées de l'UE, quel que soit le lieu où l'entreprise qui traite leurs données est établie.

Par conséquent, bien que la disparition du critère de localisation puisse être nouvelle dans le domaine du droit pénal, il ne s'agit pas d'un changement majeur du point de vue de la protection des données. En outre, le CEPD souligne également qu'un lien est maintenu avec le territoire de l'UE étant donné que seuls les fournisseurs de services offrant des services dans l'Union relèvent du champ d'application des propositions et que le fait que les demandes ne peuvent être adressées que dans le cadre d'enquêtes pénales implique un lien avec l'UE (soit parce que le délit a été commis sur le territoire d'un État membre, soit parce que la victime ou l'auteur de l'infraction était citoyen d'un État membre).

Si la disparition du critère de localisation devait maintenant être appliquée en droit pénal, la question la plus importante pour le Comité européen de la protection des données est de savoir comment faire en sorte qu'une telle évolution ne porte pas préjudice à la protection des données et aux garanties procédurales en matière pénale prévues pour les personnes concernées et des fournisseurs de services sollicités. De ce point de vue, le CEPD rappelle que, au sein de l'UE, les garanties procédurales ont été, au moins partiellement, harmonisées et doivent se conformer à la Convention européenne des droits de l'homme. On peut donc soutenir que la disparition des critères de localisation aurait probablement des conséquences plus limitées lorsque les éléments de preuve sont recherchés dans un contexte intra UE que dans la situation inverse, où les autorités de pays tiers demandent des données à des entreprises établies dans l'UE dans les mêmes conditions que celles énoncées dans le projet de règlement relatif aux preuves électroniques. En effet, le CEPD s'inquiète en particulier du fait que puissent en résulter des situations plus problématiques. Dans ce contexte, les autorités d'un pays tiers où des garanties procédurales différentes et potentiellement moins strictes s'appliquent dans le domaine du droit pénal pourraient avoir accès à des données qui seraient protégées par des garanties supplémentaires dans l'UE. De ce point de vue, le CEPD rappelle ses préoccupations quant au risque de double standard et à un affaiblissement des droits fondamentaux lorsque les fournisseurs de services et les personnes concernées ne bénéficient pas des garanties procédurales prévues par le droit de l'UE si la demande émane d'une autorité d'un pays tiers.

[17] Voir l'article 3, en particulier le paragraphe 2.
[18] Voir l'article 27.

En outre, étant donné que ce nouveau chef de compétence «quel que soit le lieu où se trouvent les données» s'accompagne d'une procédure reposant principalement sur des demandes directes d'autorités compétentes adressées aux fournisseurs de services, le CEPD craint que des garanties en matière de protection des données ne puissent être appliquées par des entreprises privées recevant des demandes et qui ne sont pas liées par un instrument juridique tel qu'un traité d'entraide judiciaire, qui régissent traditionnellement les échanges de données entre les autorités judiciaires et prévoyant des garanties. En particulier, dans le contexte des traités d'entraide judiciaire, les garanties minimales en matière de protection des données prévoient par exemple des obligations de confidentialité et le principe de spécificité qui implique que les données ne seront pas traitées pour une autre finalité.

C'est pourquoi le CEPD rappelle a minima que l'application des garanties prévues par la directive 2016/680 devraient être rendues possible, y compris en ce qui concerne les transferts de données, et en particulier l'article 39 dans le cas où le fournisseur de services serait établi dans un pays tiers sans décision d'adéquation dans ce domaine. En particulier, le CEPD souligne que cette disposition oblige notamment à informer l'autorité de protection des données compétente dans l'État membre de l'autorité émettrice de la ou des injonction(s) et à documenter le transfert, y compris en ce qui concerne la justification de l'inefficacité ou du caractère inapproprié d'un transfert vers l'autorité compétente du pays tiers.

4. La notion de «fournisseurs de services» devrait être limitée ou complétée par des garanties supplémentaires pour les droits des personnes concernées

En ce qui concerne les fournisseurs de services, le Comité européen de protection des données se félicite de la définition large qui permet d'inclure à la fois les services de communication et les services OTT (Over-The-Top, par contournement), car tous ces services sont équivalents sur le plan fonctionnel et les mesures prévues pourraient donc avoir une incidence similaire sur le droit à la vie privée et sur le droit au secret des communications, comme souligné dans la déclaration du groupe de travail « Article 29 » et précédemment dans l'avis 01/2017 concernant la proposition de règlement sur la vie privée et les communications électroniques. En effet, la proposition de règlement concernant les preuves électroniques couvre les fournisseurs de services offrant des services de communications électroniques tels qu'ils sont définis à l'article 2, paragraphe 4, de la directive établissant le code des communications électroniques européen, des services de la société de l'information tels qu'ils sont définis à l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 «pour lesquels le stockage de données est un élément déterminant du service fourni à l'utilisateur, y compris les réseaux sociaux, les marchés en ligne facilitant les transactions entre leurs utilisateurs et autres fournisseurs de services d'hébergement» ou un nom de domaine internet et des services de numérotation IP « tels que les fournisseurs d'adresses IP, les registres de noms de domaine, les bureaux d'enregistrement de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire associés »[19].

Toutefois, un fournisseur de services étant défini par la proposition de règlement comme «toute personne physique ou morale qui fournit une ou plusieurs des catégories de services suivants», le CEPD craint que cet instrument couvre à la fois les responsables du traitement et les sous-traitants au sens du RGPD. En effet, dans la mesure où la notion de «proposer des services» telle qu'elle est définie à

[19] Article 2, paragraphe 3, point c) de la proposition de règlement relatif aux preuves électroniques.

l'article 2, paragraphe 4, de la proposition de règlement, couvre à la fois la possibilité pour les personnes physiques ou morales d'un ou de plusieurs États membres d'utiliser les services énumérés et l'existence d'un lien important avec le ou les États membres en question, ces activités comprennent les activités effectuées par un sous-traitant pour le compte d'un responsable du traitement, comme le stockage des données, par exemple.

Par conséquent, le CEPD craint que, en l'absence de limitations aux seuls fournisseurs de services agissant en tant que responsables du traitement au sens du RGPD et en l'absence de toute obligation spécifique du sous-traitant d'informer le responsable du traitement lorsqu'ils reçoivent une injonction de production ou de conservation de données, les droits des personnes concernées puissent être contournés. Cela est d'autant plus le cas dans la mesure où, dans le contexte d'éventuelles obligations contradictoires empêchant le destinataire de signifier les injonctions reçues, les autorités judiciaires sont également encouragées, dans la proposition de règlement elle-même, à s'adresser à l'acteur le plus approprié, indépendamment des règles de protection des données applicables, d'autant que toute donnée pourrait être demandée, et pas seulement les données à caractère personnel qui sont assujetties au RGPD[20].

En application du RGPD, un sous-traitant n'agit que sur instruction du responsable du traitement. Il incombe donc au responsable du traitement de veiller au respect des droits des personnes concernées et de leur fournir les informations pertinentes, notamment en ce qui concerne les destinataires de leurs données, par exemple dans le cadre de l'exercice de leur droit d'accès. Le sous-traitant ne recevra pas ces demandes de personnes concernées et ne sera pas en mesure d'y répondre, sauf demande expresse du responsable du traitement de le faire.

Par conséquent, à moins que leurs droits n'aient été limités en application du RGPD, le CEPD souligne que les personnes concernées qui bénéficient de l'application du RGPD pourraient ne pas être en mesure d'exercer leurs droits de manière efficace si le responsable du traitement ne peut pas fournir des informations complètes. Le CEPD relève également que la probabilité d'absence d'information est encore plus élevée quand aucune obligation spécifique n'est imposée au sous-traitant d'informer le responsable du traitement lorsque les données demandées ont trait à des personnes concernées qui ne bénéficient pas de la protection accordée par le RGPD. En effet, les autorités judiciaires qui demandent les données n'auront pas nécessairement l'obligation d'informer les personnes concernées de leur propre traitement ultérieur dans ce cas. Le CEPD demande donc de limiter le champ d'application aux responsables du traitement au sens du RGPD ou d'introduire une disposition précisant que si le fournisseur de services destinataire des injonctions n'est pas le responsable du traitement des données, il doit en informer ce dernier.

5. Les notions d'«établissement» et de «représentant légal» dans le contexte de ces propositions devraient être clairement distinguées des mêmes notions dans le contexte du RGPD

Compte tenu de l'inapplicabilité du critère de localisation en ce qui concerne les données, les destinataires des injonctions de production et de conservation relevant du champ d'application du règlement proposé sont limités aux fournisseurs de services offrant des services dans l'Union, établis ou non dans l'UE, avec l'obligation de désigner un représentant légal, conformément aux règles

[20] Article 7, paragraphes 3 et 4.

proposées dans la proposition de directive. Ces notions d'«établissement» et de «représentant légal» sont dès lors définies dans les projets d'instruments.

Le CEPD observe que ces notions apparaissent également dans le contexte d'autres instruments de l'UE et, en particulier, dans le contexte du RGPD. En conséquence, il convient de clarifier la définition et la délimitation de ces notions dans le contexte des propositions d'instruments et dans le contexte du RGPD.

a) Établissement

Le CEPD rappelle également que la notion d'«établissement» dans le contexte du projet de règlement ne doit pas être confondue avec la même notion dans le contexte du RGPD. En effet, aux fins du projet de règlement, la notion d'«établissement» telle qu'elle est définie à l'article 2, paragraphe 5, est plus large que dans le RGPD, car elle inclut «la poursuite effective d'une activité économique pour une durée indéterminée grâce à une infrastructure stable à partir de laquelle l'activité de fourniture de services est réalisée ou une infrastructure stable à partir de laquelle l'entreprise est gérée», que le traitement des données à caractère personnel ait lieu ou non dans le contexte des activités de cet établissement. Ainsi, si l'«établissement» au sens du RGPD est sans aucun doute inclus dans l'établissement tel que défini dans le projet de règlement, le contraire n'est sans doute pas vrai.

Le CEPD met donc en garde contre le fait que les établissements de fournisseurs de services au sens du projet de règlement n'impliquent pas nécessairement que les conditions d'application du RGPD conformément à l'article 3, paragraphe 1, sont remplies. Dans ce contexte, les responsables du traitement et les sous-traitants sont donc invités à vérifier si l'applicabilité du RGPD ne découle pas de l'article 3, paragraphe 2, qui impliquerait la désignation d'un représentant légal dans l'UE et l'absence de mécanisme de guichet unique.

b) Représentant légal

Dans sa déclaration, le groupe de travail « Article 29 » a souligné le fait qu'il convenait d'éviter toute confusion entre l'obligation de désigner un représentant légal en vertu de l'article 27 du RGPD et le représentant légal prévu par le projet de règlement relatif aux preuves électroniques.

Le projet de règlement étant désormais disponible, le CEPD souhaite rappeler ces recommandations et souligner en particulier que selon lui, le représentant légal au sens du projet de directive sur la désignation d'un représentant légal dans le contexte des propositions relatives aux preuves électroniques doit être désigné dans tous les cas, être investi de fonctions spécifiques, indépendamment d'un mandat donné par le fournisseur de services, avoir le pouvoir de répondre aux demandes et d'agir au nom du fournisseur de services et qu'il doit avoir une responsabilité plus importante que le représentant légal du RGPD.

En outre, le CEPD souligne que l'obligation de désigner un représentant légal dans tous les cas dans le cadre des projets de propositions relatives aux preuves électroniques, que le fournisseur de services soit établi dans l'UE ou non, la possibilité de désigner plusieurs représentants légaux pour le même fournisseur de services en vertu du projet de directive concernant les preuves électroniques et l'obligation de notifier la désignation du représentant légal aux autorités des États membres diffèrent de ce qui figure dans le RGPD, qui ne prévoit pas cette obligation de notifier le représentant légal désigné, mais en revanche prévoit des exemptions à la désignation et des responsabilités limitées pour le représentant légal désigné.

Par conséquent, compte tenu des différences importantes en termes de rôle, de responsabilité et de relations avec les autres établissements du fournisseur de services dans un cas et avec le responsable du traitement ou le sous-traitant dans l'autre, le CEPD recommande que, lorsqu'un fournisseur de services n'est pas établi dans l'UE, mais est soumis au RGPD conformément à l'article 3, paragraphe 2, et au règlement relatif aux preuves électroniques, deux représentants légaux distincts soient désignés, chacun ayant des fonctions clairement distinctes selon l'instrument sur la base duquel il est désigné.

6. Nouvelles catégories de données

La proposition de règlement définit différentes catégories de données conformément à l'article 2 : les données relatives aux abonnés, les données relatives à l'accès, les données relatives aux transactions et celles relatives au contenu. Le considérant 20 de la proposition de la Commission précise en outre que « *les catégories de données couvertes par le présent règlement comprennent les données relatives aux abonnés, les données relatives à l'accès et les données relatives aux transactions (ces trois catégories étant désignées comme les "données non relatives au contenu") et les données relatives au contenu. Cette distinction, sauf pour les données relatives à l'accès, existe dans le droit de nombreux États membres, ainsi que dans le cadre juridique actuel des États-Unis, qui permet aux fournisseurs de services de partager les données non relatives au contenu avec les autorités répressives étrangères sur une base volontaire.*»

Dans ce contexte, le CEPD souligne tout d'abord que les quatre catégories de données susmentionnées doivent être considérées comme des données à caractère personnel au regard du droit de l'UE en matière de protection des données, car elles contiennent des informations relatives à une personne physique identifiée ou identifiable, que la personne concernée soit désignée comme «abonné» ou comme «utilisateur» dans la proposition de règlement. De la même manière, il convient de noter que la «preuve électronique» au sens de l'article 2, paragraphe 6, de la proposition de la Commission couvre les quatre catégories de données et correspond donc des données à caractère personnel. Par conséquent, plutôt que de fixer les règles d'accès aux preuves, définies et qualifiées conformément à la législation et aux procédures judiciaires nationales, la proposition de règlement prévoit de nouvelles conditions de fond et de procédure concernant l'accès aux données à caractère personnel.

Bien que le règlement proposé établisse de nouvelles sous-catégories de données à caractère personnel pour lesquelles différentes conditions d'accès procédurales s'appliquent, le CEPD rappelle que, conformément à la jurisprudence pertinente de la Cour de justice, pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, 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.

En outre, le CEPD rappelle que, en ce qui concerne les «données hors contenu», qui couvrent les données relatives aux abonnés, les données relatives à l'accès et les données relatives aux transactions au titre de la proposition de la Commission, la Cour de justice de l'Union européenne a établi, dans son arrêt dans les affaires jointes C-203/15 et C-698/15, Tele2 *Sverige AB*, que les métadonnées telles que les données relatives au trafic et les données de localisation fournissent les moyens d'établir le profil des personnes concernées, information qui n'est pas moins sensible, au regard du droit au respect de la vie privée, que le contenu même des communications[21].

[21] Arrêt de la Cour de justice du 21 décembre 2016, point 99.

Comme déjà indiqué dans la déclaration du groupe de travail « Article 29 » du 29 novembre 2017 concernant la protection des données et les aspects relatifs au respect de la vie privée de l'accès transfrontalier aux preuves électroniques, le Comité européen de protection des données réitère ses doutes et ses inquiétudes en ce qui concerne l'actuelle délimitation entre les «données hors contenu» et les données relatives au contenu, ainsi qu'en ce qui concerne les quatre catégories de données à caractère personnel établies dans la proposition de règlement. En effet, les quatre catégories proposées ne semblent pas clairement délimitées et la définition des «données relatives à l'accès» reste encore vague par rapport aux autres catégories. Le CEPD regrette donc que l'analyse d'impact et la proposition de la Commission n'aient pas justifié davantage le bien-fondé de la création de ces nouvelles sous-catégories de données à caractère personnel et exprime ses préoccupations quant aux différents niveaux de garanties en lien avec les conditions de fond et de procédure permettant l'accès aux catégories de données à caractère personnel, en particulier en raison des difficultés pratiques pour évaluer à quelle catégorie de données appartiennent les données demandées dans certains cas. Par exemple, les adresses IP pourraient être classées à la fois comme données relatives aux transactions et comme données relatives aux abonnés.

Dans ce contexte, le CEPD rappelle également qu'au considérant 14 de sa proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (règlement «vie privée et communications électroniques»), la Commission estime que «[l]es données de communications électroniques devraient être définies de façon suffisamment large et neutre du point de vue technologique pour englober toute information concernant le contenu transmis ou échangé (contenu des communications électroniques) et toute information concernant l'utilisateur final de services de communications électroniques traitée aux fins de la transmission, la distribution ou l'échange de ce contenu, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que le lieu, la date, l'heure, la durée et le type». Dans la mesure où le cadre actuel et futur de la protection de la vie privée dans le secteur des communications électroniques, ainsi que les limitations au droit à la vie privée, s'appliqueront aux règles régissant l'accès des services répressifs aux preuves électroniques, le CEPD recommande d'inclure dans la proposition de règlement sur l'accès aux preuves électroniques une définition plus large des données relatives aux communications électroniques, afin de garantir que les garanties et conditions appropriées d'accès couvrent de manière uniforme tant les «données hors contenu» que les «données relatives au contenu».

7. Analyse des procédures pour les injonctions européennes de conservation et de production

D'une manière générale, la procédure à suivre pour émettre une injonction de production ou de conservation paraît être la suivante:

- en fonction du type de données demandées et du type d'injonction, l'autorité judiciaire compétente - l'autorité émettrice - émet l'injonction conformément aux (quelques) conditions énoncées aux articles 5 et 6, l'envoie, au moyen d'un certificat harmonisé, au représentant légal du fournisseur de services ou à l'un de ses établissements dans l'UE - le destinataire.
- Dès réception du certificat, le destinataire doit exécuter l'injonction, c'est-à-dire qu'il transmet les données dans un délai de 10 jours ou de 6 heures en cas d'urgence, ou qu'il les conserve jusqu'à 60 jours, sauf si c'est impossible parce que le certificat est incomplet ou en cas de force majeure ou d'impossibilité de fait pour le destinataire, ou parce que le destinataire refuse de

l'exécuter en raison d'obligations contradictoires, soit au regard des droits fondamentaux ou des intérêts fondamentaux d'un pays tiers ou pour d'autres motifs.

- Si le destinataire ne s'est pas conformé à l'injonction reçue sans fournir de motifs acceptés par l'autorité émettrice, des procédures sont prévues pour faire exécuter les injonctions par une autorité d'exécution compétente dans l'État membre où le fournisseur de services est représenté ou établi, à moins que des motifs de refus limités ne s'appliquent et que l'autorité d'exécution ne s'oppose à la reconnaissance ou à l'exécution de l'injonction.
- Si le destinataire a émis une objection motivée à l'injonction fondée sur des obligations contradictoires, l'autorité émettrice saisit la juridiction compétente de son État membre, qui est alors chargée d'évaluer l'existence d'un conflit éventuel et de maintenir l'injonction en l'absence de conflit. En cas de conflit, la juridiction compétente s'adresse aux autorités centrales du pays tiers, par l'intermédiaire de ses autorités centrales nationales, avec un délai de réponse sous 15 jours, qui peut être prolongé de 30 jours sur demande motivée, en cas d'obligations contradictoires concernant les droits fondamentaux ou les intérêts fondamentaux d'un pays tiers, ou décide elle-même si l'injonction doit être maintenue ou retirée pour tout autre motif de refus invoqué par son destinataire.
- Sans préjudice des recours disponibles dans le cadre du RGPD et de la directive en matière de protection des données dans le domaine répressif, les personnes dont les données ont été obtenues au moyen d'une injonction de production ont également le droit à un recours effectif à l'encontre de cette injonction.

Le CEPD a évalué les procédures prévues et les garanties fournies dans le projet de règlement pour encadrer les différentes étapes et, concernant chacun des aspects présentés ci-après, il recommande les garanties et modifications suivantes.

a) Les seuils d'émission des injonctions devraient être relevés et les injonctions devraient être émises ou autorisées par les tribunaux

En ce qui concerne les conditions d'émission des injonctions, le CEPD se félicite que, par principe, des garanties plus élevées soient prévues pour l'accès aux données relatives aux transactions ou relatives au contenu. Toutefois, il note que, en raison de l'absence d'harmonisation complète des sanctions pénales entre les États membres, la référence aux « infractions pénales passibles dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans »[22] implique toujours des seuils différents et des divergences dans la protection de leurs données pour les personnes concernées au sein de l'UE.

En outre, le CEPD souligne que, compte tenu en particulier de la définition large des données relatives aux abonnés, le seuil prévu semble assez bas pour les injonctions de conservation et pour les injonctions de production concernant les données relatives aux abonnés ou à l'accès, car toutes les infractions pénales peuvent en principe justifier l'émission de telles injonctions. De même, les autorités habilitées à émettre de telles injonctions sont plus limitées dans le contexte des injonctions de production concernant des données relatives aux transactions ou au relatives au contenu que pour l'émission d'injonctions de conservation ou d'injonctions de production visant à produire des données relatives aux abonnés ou à l'accès, puisque les procureurs ne peuvent émettre ou autoriser que ces

[22] Voir l'article 5, paragraphe 3, point a).

dernières injonctions, alors que tout juge, tribunal ou juge d'instruction peut émettre ou autoriser tout type d'injonction.

En particulier, le CEPD regrette que le seuil le plus bas permettant aux autorités répressives de demander l'accès aux données relatives aux abonnés et aux données relatives à l'accès pour les infractions pénales s'appuie sur une interprétation «a contrario» de la jurisprudence de la Cour de justice (qui se concentre sur les autres données) afin d'opérer des distinctions quant aux garanties à accorder. En effet, la Cour de justice a spécifiquement souligné que, en ce qui concerne les données relatives au trafic et les données de localisation, l'accès des autorités compétentes doit être limité aux seules fins de lutte contre la criminalité grave[23]. Le CEPD pourrait admettre que la proposition offre la possibilité de demander l'accès à des informations très basiques qui permettraient juste d'identifier une personne sans révéler des données de communication sans autorisation préalable d'un tribunal. Il déplore toutefois l'interprétation générale « a contrario » faite de cet arrêt par la Commission et demande l'introduction de garanties plus rigoureuses afin de limiter les motifs d'accès à d'autres données relatives aux abonnés et à des données relatives à l'accès. Le CEPD suggère de limiter l'accès à ces données soit à une liste d'infractions prévues dans le projet de règlement, ou tout au moins aux « infractions pénales graves », compte tenu du seuil d'autorisation préalable plus bas qui est prévu pour ces données.

En outre, le CEPD souligne que cette interprétation « a contrario » conduit également au fait que la proposition donne la possibilité aux procureurs d'émettre des injonctions ou d'en autoriser l'émission. Le CEPD est d'avis que, à l'exception des demandes portant sur des informations très basiques qui permettraient seulement d'identifier une personne sans révéler des données de communication, cela constitue un recul par rapport à la jurisprudence de la Cour de justice concernant l'accès aux données de communication. En effet, dans sa jurisprudence relative à l'accès aux données de communication à des fins répressives, la Cour de justice a limité la possibilité de fournir cet accès, entre autres critères, et « *sauf cas d'urgence dûment justifiés* »[24], à « *un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante* », «*à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénale*. »[25]

Le CEPD rappelle que la notion de « juridiction » est une notion autonome du droit de l'UE, et que la Cour de justice a constamment souligné et rappelé les critères à satisfaire pour avoir la qualité de juridiction, dont les critères d'indépendance[26], ce qui ne semble pas être le cas des procureurs, comme le rappelle également la CEDH dans sa jurisprudence[27].

Par conséquent, l'article 4, paragraphe 1, points a) et b), et l'article 3, points a) et b), mettent en place des procédures qui réduisent sensiblement les garanties pour les données relatives aux abonnés et les données relatives à l'accès dans la mesure où un procureur seul pourra demander des données, sans autre contrôle de l'autorité de l'État où se trouvent les données demandées ou de l'autorité où se trouvera le représentant légal de la société à laquelle les données sont demandées et sans autre contrôle d'une autorité administrative indépendante.

De plus, le CEPD prend note de la garantie supplémentaire prévue à l'article 5, paragraphe 2, qui limite la possibilité d'émettre une injonction lorsqu'il existe une mesure similaire pour la même infraction

[23] Voir l'affaire C-203/15 - Point 125
[24] Voir l'affaire C-203/15 - point 120
[25] Voir les affaires jointes C-293/12 et C-594/12 - point 62
[26] Voir, par exemple, l'affaire C-203/14
[27] Voir, par exemple, l'affaire Moulin c./France du 23 novembre 2010

pénale dans une situation nationale comparable. Il met toutefois en garde contre l'effet contre-productif d'une telle disposition : plutôt que de fournir des garanties supplémentaires, cette disposition semble encourager les États membres à étendre leurs possibilités nationales pour demander la production de données relatives aux abonnés ou à l'accès afin de garantir que les injonctions de production peuvent être émises dans le cadre de ce règlement.

b) Les délais fixés pour la transmission des données devraient être justifiés

Le CEPD relève qu'il convient de répondre aux injonctions de production dans les 10 jours au plus tard à compter de la réception du certificat, à moins que l'autorité émettrice ne fournisse des raisons pour une divulgation anticipée, et au plus tard dans les 6 heures en cas d'urgence, comme prévu à l'article 9, paragraphes 1 et 2.

Toutefois, le CEPD ne voit aucun critère encadrant l'obligation qui incombe aux autorités de démontrer l'urgence à produire des données, même a posteriori, afin de permettre un contrôle éventuel de l'utilisation de cette procédure très rapide, tandis qu'un délai de six heures est susceptible d'impliquer un contrôle très superficiel avant la production des données, voire l'absence de tout contrôle de la part du fournisseur de services. En effet, l'analyse d'impact souligne la nécessité que les autorités compétentes accèdent à des données dans les meilleurs délais. Toutefois, les exemples fournis dans l'analyse d'impact concernent tous des éléments de preuve requis dans des cas où des délits graves ont été commis (cas de terrorisme avec otages, abus sexuels continus sur enfants), mais la justification basée sur la volatilité des éléments de preuve n'apparaît pas acceptable en l'absence d'urgence spécifique autre que cette volatilité potentielle des données. En outre, la volatilité des données ne fournit aucune autre justification quant à la proportionnalité d'accéder à des données avec moins de garanties dans ces situations dépourvues d'urgence autre que la volatilité des données.

Par ailleurs, le Comité européen pour la protection des données doute de la nécessité de prévoir un délai de six heures tout en prévoyant que ce délai ne s'appliquera pas tant que l'autorité émettrice ne fournira pas des éclaircissements supplémentaires « dans les cinq jours » dans le cas où le fournisseur de services ne pourra pas s'acquitter de son obligation.

Le CEPD demande dès lors l'inclusion dans l'analyse d'impact d'éléments supplémentaires justifiant la nécessité de ces délais dans les cas où le délit commis ou poursuivi n'est pas grave, et à moins que ces éléments détaillés ne soient fournis, de critères explicites pour justifier l'urgence lorsque des EPOC sont émises. Par exemple, le même modèle que celui qui figure dans la directive concernant la décision d'enquête européenne en matière pénale pourrait être prévu. La directive concernant la décision d'enquête européenne en matière pénale prévoit un délai plus court lorsqu'il est justifié « en raison de délais de procédure, de la gravité de l'infraction ou d'autres circonstances particulièrement urgentes » (voir l'article 12, paragraphe 2), ou un délai de 24 heures pour se prononcer sur les mesures provisoires (voir l'article 32, paragraphe 2). En effet, l'analyse d'impact du projet de règlement ne contient pas d'éléments détaillés pour justifier la raison pour laquelle ces délais ne sont pas efficaces, les seuls éléments soulignés étant que le nombre de demandes envoyées surcharge les autorités judiciaires destinataires qui ne peuvent respecter les délais.

c) Les injonctions européennes de production et de conservation ne doivent pas être utilisées pour demander des données d'une personne concernée d'un autre État membre sans au moins en informer les autorités compétentes dudit État membre, en particulier pour les données relatives au contenu

Le CEPD rappelle que dans les instruments existants c'est une coopération judiciaire qui est prévue et, partant, que des garanties supplémentaires sont également prévues, en particulier afin de contrôler la nécessité et la proportionnalité des demandes, et souligne que ces garanties sont d'autant plus justifiées dans les cas où les données demandées sont des données relatives au contenu qui impliquent davantage de limitations des droits des personnes concernées à la protection de leurs données à caractère personnel et de leur vie privée. À cet égard, le CEPD rappelle que la directive concernant la décision d'enquête européenne en matière pénale prévoit également la possibilité d'intercepter des télécommunications avec l'assistance technique d'un autre État membre (article 30), ainsi que l'obligation de notification de toute interception des données à l'autorité compétente d'un autre État membre où aucune assistance n'est nécessaire lorsque la personne concernée par l'interception se trouve ou se trouvera sur le territoire de l'État membre notifié (voir l'article 31).

Le CEPD ne voit aucune justification à la procédure prévue dans le projet de règlement concernant les preuves électroniques permettant la production de données relatives au contenu sans la participation au moins des autorités compétentes de l'État membre dans lequel se trouve la personne concernée.

d) Les injonctions européennes de conservation ne seront pas utilisées pour contourner les obligations de conservation de données qui incombent aux fournisseurs de services

Le CEPD souligne que l'objectif premier des injonctions européennes de conservation est d'empêcher que des données soient supprimées.

Si le CEPD reconnaît que dans certains cas de telles injonctions peuvent être nécessaires et proportionnées, il déplore le manque de garanties entourant l'émission de ces injonctions. En particulier, le CEPD recommande que lorsque des injonctions de conservation sont adressées pour des données spécifiques uniquement, alors que le projet de règlement semble autoriser des demandes générales, et que lorsque ces injonctions sont émises pour des données dont la suppression est prévue conformément au principe de conservation des données, l'injonction ne doit jamais servir de base permettant au fournisseur de services de traiter les données après la date initiale de leur suppression. En d'autres termes, les données doivent être « gelées ».

En outre, le lien entre l'injonction de conservation et la demande ultérieure de production des données, qu'il s'agisse d'une injonction européenne de production, d'une demande de décision d'enquête européenne ou d'une demande d'entraide judiciaire, doit être renforcé, de manière à garantir que les injonctions européennes de conservation ne sont émises que lorsque l'autre demande est certaine (et pas seulement envisagée en tant que possibilité), et que lorsque l'autre demande est refusée, l'injonction de conservation expire également, sans devoir attendre 60 jours[28] si la demande ultérieure est refusée plus tôt.

e) Confidentialité et information de l'utilisateur

Le CEPD observe qu'un article spécifique[29] concernant la confidentialité des injonctions notifiées a été introduit dans le projet de règlement. Afin d'éviter toute confusion et tout quiproquo avec le droit à la protection des données, le CEPD rappelle que, bien que le RGPD prévoie que les limitations aux droits des personnes concernées aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales doivent être prévues par la loi et

[28] Voir l'article 10, paragraphe 1.
[29] Voir l'article 11.

être dès lors accessibles au public[30], et que ces mesures législatives doivent contenir des dispositions spécifiques quant au droit des personnes concernées à être informées de la restriction, sauf si cela peut nuire à la finalité de la restriction[31], il ne prévoit pas l'obligation d'informer individuellement les personnes concernées de chaque demande d'accès faite par les autorités répressives.

Toutefois, dans le même temps, le CEPD rappelle que la directive sur la protection des données prévoit ce droit d'information des personnes concernées par les autorités compétentes elles-mêmes, à moins que ce droit n'ait été limité, pour toute personne concernée sans limiter ce droit aux seules personnes concernées résidant sur le territoire de l'UE.

f) Procédure de mise en œuvre d'une injonction lorsque le fournisseur de services refuse de la mettre en œuvre

Le CEPD observe que l'article 14 du projet de règlement prévoit une procédure visant à assurer la mise en œuvre d'une injonction lorsque le destinataire ne s'y conforme pas, sur la base d'une coopération judiciaire entre l'autorité d'émission et une autorité compétente dans l'État de mise en œuvre de l'injonction.

Toutefois, il apparaît que cette procédure ne permet pas à l'autorité chargée de la mise en œuvre de refuser la mise en œuvre de l'injonction transmise pour d'autres motifs que des motifs purement procéduraux (identiques à ceux du destinataire, concernant principalement le manque d'informations fournies ou l'impossibilité factuelle de fournir les données), parce que les données concernées sont protégées par une immunité ou un privilège selon son droit national ou parce que leur divulgation pourrait affecter ses intérêts fondamentaux, par exemple en matière de sécurité ou de défense nationales[32].

Le CEPD réitère donc ses préoccupations quant à la suppression de tout double contrôle de l'injonction transmise par l'autorité compétente destinataire par rapport aux autres instruments. Même le motif de refus de mettre en œuvre une injonction au motif qu'elle violerait la Charte semble plus élevé que le seuil classique relatif à une violation des droits fondamentaux de la personne concernée. Par conséquent, suivant l'exemple du mandat d'arrêt européen, qui prévoit des motifs de refus obligatoires ainsi que facultatifs, ou au moins de la directive concernant la décision d'enquête européenne en matière pénale, qui stipule généralement que la présomption selon laquelle « la création d'un espace de liberté, de sécurité et de justice dans l'Union est fondée sur la confiance mutuelle et la présomption que les autres États membres respectent le droit de l'Union et, en particulier, les droits fondamentaux » est réfragable[33], le projet de règlement doit au moins prévoir la dérogation classique minimale selon laquelle, s'il existe des motifs substantiels de croire que la mise en œuvre d'une injonction conduirait à une violation du droit fondamental de la personne concernée et que l'État chargé de la mise en œuvre ne s'acquitterait pas de ses obligations concernant la protection des droits fondamentaux reconnus dans la Charte, la mise en œuvre de l'injonction doit être refusée.

g) Mise en œuvre des injonctions et obligations contradictoires dans la législation des pays tiers (articles 15 et 16)

[30] Voir l'article 23, paragraphe 1, point d)
[31] Voir l'article 23, paragraphe 2, point h)
[32] Voir l'article 14, paragraphe 2.
[33] Voir le considérant 19 de la directive concernant la décision d'enquête européenne en matière pénale

Le CEPD se félicite de la possibilité offerte par le projet de règlement aux destinataires d'injonctions de refuser une telle injonction au motif qu'elle serait contraire aux droits fondamentaux, dans la mesure où elle vise à fournir des garanties en cas d'obligations légales contradictoires. Il juge également essentiel que la proposition prévoie la consultation des autorités des pays tiers, au moins en cas de conflit, ainsi que l'obligation de lever l'injonction lorsque l'autorité d'un pays tiers soulève une objection.

Par conséquent, la procédure prévue pour refuser la mise en œuvre d'une injonction sur la base d'obligations contradictoires découlant des législations de pays tiers devrait être considérablement améliorée.

Premièrement, le CEPD observe que le projet de règlement confie à une société privée, en tant que destinataire d'une injonction de production, le soin d'évaluer si cette injonction est ou non en conflit avec les législations applicables d'un pays tiers interdisant la divulgation des données demandées. La société doit fournir une objection motivée incluant toutes les informations pertinentes sur la législation du pays tiers, son applicabilité en l'espèce et la nature des obligations contradictoires.

Plus important encore, le CEPD est préoccupé par le fait que lorsqu'une telle objection est soulevée, seule la juridiction compétente de l'État membre de l'autorité émettrice évalue s'il existe ou non un conflit, puisque ce n'est que lorsque la juridiction constate un conflit qu'elle doit entrer en contact avec les autorités du pays tiers. La juridiction compétente de l'UE est donc habilitée à interpréter de manière définitive la législation d'un pays tiers dans ce contexte, sans pour autant être un spécialiste sur le fond. Le CEPD considère que l'obligation de consulter les autorités compétentes du pays tiers est donc trop limitée dans la proposition actuelle. Dans le domaine de la protection des données, le CEPD attire l'attention du législateur sur le fait que, dans le cas où une juridiction compétente d'un pays tiers interpréterait le RGPD afin de déterminer s'il est contraire à ses propres exigences, les autorités de l'UE chargées de la protection des données et les juridictions compétentes resteraient compétentes pour évaluer la légalité du transfert sur la base d'une décision d'une juridiction ou d'un tribunal ou d'une décision d'une autorité administrative d'un pays tiers exigeant un transfert ou une divulgation des données à caractère personnel dans le cadre du RGPD[34].

En outre, le CEPD souligne que l'évaluation de la législation du pays tiers par la juridiction compétente de l'État requérant de l'UE doit être fondée sur des éléments objectifs et qu'il est préoccupé par les critères à prendre en compte par la juridiction compétente pour apprécier la législation du pays tiers en vertu de l'article 15, paragraphe 4, et de l'article 16, paragraphe 5, point a), du projet de règlement. En effet, la juridiction doit évaluer si « la législation du pays tiers, plutôt que d'être destinée à protéger les droits fondamentaux ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, vise manifestement à protéger d'autres intérêts ou vise à protéger des activités illégales de demandes d'application de la loi dans le contexte d'enquêtes criminelles » ou si « l'intérêt protégé par la législation pertinente du pays tiers, y compris l'intérêt du pays tiers d'empêcher la divulgation des données ». Par exemple, bien qu'en principe, cette évaluation devrait appeler une appréciation fondée sur les preuves à la lumière de toutes les informations disponibles, compte tenu de l'incidence potentielle de cette décision, à tout le moins, le libellé (« vise à ») semble peu clair et doit être adapté (« a pour objectif/but de »).

Le CEPD regrette que le seul cas où les autorités d'un pays tiers seraient consultées et pourraient s'opposer à la mise en œuvre d'une injonction de production soit celui où cette juridiction compétente de l'UE considérerait qu'il existe un conflit pertinent, transmettrait tous les éléments aux autorités

[34] Voir l'article 48 du RGPD.

centrales du pays tiers concerné et où l'autorité centrale de ce pays tiers s'y opposerait dans les brefs délais de 50 jours maximum (15 jours, éventuellement prolongés de 30 jours, et après un dernier rappel possible donnant 5 jours supplémentaires). Dans tous les autres cas, la juridiction compétente serait en mesure de confirmer l'injonction de production et d'infliger une sanction pécuniaire au fournisseur de services qui refuse de mettre en œuvre l'injonction. Par conséquent, le CEPD craint que les juridictions compétentes de l'UE n'aient pas une obligation plus générale de consulter les autorités compétentes des pays tiers concernés afin de garantir que la procédure veille plus systématiquement à ce que les arguments des deux parties soient pris en compte et que plus de respect encore soit accordée aux législations des pays tiers.

Comme déjà souligné dans la déclaration du groupe de travail « Article 29 » et ci-dessus, le CEPD rappelle qu'une attention particulière doit être accordée à l'adoption par les pays tiers d'instruments similaires susceptibles d'affecter les droits des personnes concernées dans l'UE et leur droit au respect de leur vie privée, et notamment au risque que des instruments similaires entrent en conflit direct avec la législation de l'UE en matière de protection des données.

En outre, le CEPD souligne que la juridiction compétente de l'État membre de l'autorité émettrice pourrait même ne pas être la juridiction compétente pour mettre en œuvre l'injonction prévue à l'article 14 du projet de règlement, ce qui augmenterait encore le risque de procédures contradictoires et l'absence de contre-vérifications dans une situation de conflits de lois. Cela vient du fait que, dans certains cas, trois États pourraient être impliqués : l'État de l'autorité qui a émis l'injonction, le pays tiers du fournisseur de services et l'État membre où se trouve le représentant légal du fournisseur de services dans l'UE et où l'injonction devrait être mise en œuvre. Par conséquent, selon la procédure actuellement prévue, la juridiction de l'autorité requérante de l'État membre A pourrait faire sa propre interprétation de la législation du pays tiers B du fournisseur de services sans demander l'avis des autorités de ce pays tiers (alors qu'elles se seraient opposées à l'injonction) et demander à une juridiction d'un autre État membre C de mettre en œuvre son injonction sans aucune possibilité d'objection.

Par ailleurs, le CEPD se félicite également de l'introduction de recours spécifiques contre les injonctions de production, en plus des recours prévus dans le RGPD et dans la directive en matière de protection des données dans le domaine répressif. Le groupe de travail « Article 29 » a déjà appelé à l'introduction de telles sauvegardes dans sa précédente déclaration. Toutefois, le CEPD déplore que de tels recours ne soient pas également prévus à l'encontre des injonctions de conservation, car ces dernières peuvent également entraîner des limitations aux droits fondamentaux des personnes dont les données sont conservées. En effet, les injonctions de conservation peuvent avoir pour effet de conserver les données plus longtemps qu'elles ne l'auraient été conformément aux règles en matière de protection des données. Par conséquent, l'injonction de conservation entraîne en soi une limitation des droits fondamentaux de la personne concernée, dont la justification doit faire l'objet d'un réexamen et de recours spécifiques, en particulier dans les cas où l'injonction de conservation aura été rendue en même temps qu'une injonction de production pour obtenir les données. Comme le recommande le groupe de travail « Article 29 » dans sa déclaration, il convient de prévoir des recours juridiques au moins équivalents à ceux qui sont mis à disposition dans une affaire nationale.

h) Sécurité des transferts de données lors de la réponse à une injonction

Le CEPD observe que la proposition de règlement ne prévoit que des injonctions à adresser à des destinataires établis au sein de l'Union européenne et ne prévoit donc pas de canal spécifique pour le transfert de données entre les destinataires et les fournisseurs de services situés hors de l'Union européenne.

Bien que le CEPD se félicite de l'absence de nouvelles dérogations au cadre général de l'UE en matière de protection des données, il rappelle que toute injonction adressée à un destinataire qui impliquerait alors un transfert hors de l'UE devrait respecter le cadre juridique prévu par le RGPD. En effet, le contournement du cadre juridique de la coopération judiciaire, qui prévoit le respect des garanties en matière de protection des données, ne devrait pas non plus entraîner le contournement des exigences en matière de transfert de données par les destinataires des injonctions de production ou de conservation pour se conformer à ces injonctions.

En outre, si le CEPD se félicite de l'absence de disposition imposant l'obligation de décrypter les données cryptées[35], il est préoccupé par le fait que les propositions ne prévoient pas d'obligation spécifique pour les destinataires d'évaluer l'authenticité des données produites et souligne que cette évaluation constitue également une valeur ajoutée des instruments traditionnels reposant sur la coopération judiciaire et met en garde contre les risques accrus qui pourraient se présenter aux personnes concernées en l'absence d'une telle évaluation.

Conclusions

Sur la base de cette évaluation, le CEPD souhaite adresser les recommandations suivantes aux co-législateurs :

1) La base juridique du règlement ne devrait pas être l'article 82, paragraphe 1, TFUE.
2) La nécessité d'un nouvel instrument par rapport à la directive existante concernant la décision d'enquête européenne en matière pénale ou aux accords d'entraide judiciaire devrait être mieux démontrée, notamment par une analyse détaillée des moyens moins intrusifs en ce qui concerne les droits fondamentaux tels que la modification des instruments existants ou la limitation du champ d'application de cet instrument aux injonctions de conservation en combinaison avec d'autres procédures existantes pour demander un accès aux données.
3) Le règlement devrait prévoir un délai plus long pour permettre au fournisseur de services chargé de la mise en œuvre de veiller au respect des garanties en matière de protection des droits fondamentaux.
4) Le principe de double incrimination devrait être maintenu, en particulier si les critères de localisation des données sont abandonnés afin de maintenir l'obligation de prendre en considération les garanties prévues dans les deux États concernés (l'État de l'autorité requérante et l'État où le fournisseur de services est établi).
5) Le champ d'application du règlement devrait être limité aux responsables du traitement au sens du RGPD ou bien il devrait introduire une disposition précisant que, si le fournisseur de services destinataire n'est pas le responsable du traitement des données, il doit en informer ce dernier.
6) Le règlement devrait prévoir des garanties concernant les transferts de données au cas où le fournisseur de services serait établi dans un pays tiers sans décision d'adéquation dans ce domaine ou renvoyer à la directive 2016/680 étant donné que ces garanties seront applicables.
7) Dans la mesure où la désignation obligatoire d'un représentant légal diffère de ce qui est prévu dans le RGPD, le règlement devrait préciser que le représentant légal désigné en vertu du règlement sur les preuves électroniques devrait être différent de celui désigné en vertu de l'article 3, paragraphe 2, du RGPD.

[35] Voir le considérant 19 et la page 240 de l'analyse d'impact.

8) Le règlement devrait contenir une définition plus large des données relatives aux communications électroniques afin de faire en sorte que les garanties et les conditions d'accès appropriées qui seront établies couvrent à la fois les données hors contenu et les données relatives au contenu.
9) Le règlement devrait relever les seuils d'émission des injonctions et celles-ci devraient être émises ou autorisées par les tribunaux, à l'exception des données relatives aux abonnés, à condition que la définition de cette catégorie de données soit considérablement réduite pour ne concerner que des informations très basiques permettant uniquement d'identifier une personne sans impliquer l'accès à aucune donnée de communication.
10) Le règlement devrait limiter l'accès aux données relatives aux abonnés et les données relatives à l'accès à une liste d'infractions strictement établies ou au moins aux « infractions pénales graves ».
11) Le délai fixé pour la transmission des données, en particulier en cas d'urgence, devrait être mieux justifié dans le règlement, et la possibilité d'utiliser une procédure rapide de 6 heures devrait inclure l'obligation pour les autorités requérantes de démontrer, même a posteriori, l'urgence qui déclenche le recours à cette procédure, afin de permettre un contrôle de l'utilisation de tels pouvoirs exceptionnels.
12) Il convient d'abandonner la procédure permettant la production de données relatives au contenu sans aucune intervention des autorités compétentes de l'État membre où se trouve la personne concernée.
13) Les sauvegardes entourant l'émission d'injonctions européennes de conservation devraient être améliorées dans le règlement.
14) Le règlement devrait au moins inclure la dérogation classique minimale selon laquelle, s'il y a des motifs sérieux de penser que l'application d'une injonction entraînerait une violation d'un droit fondamental de la personne concernée, ce qui conduirait l'État chargé de l'application à ne pas respecter ses obligations concernant la protection des droits fondamentaux reconnus dans la Charte, la mise en œuvre de cette injonction devrait être refusée.
15) Le règlement devrait prévoir une obligation plus large de consulter les autorités compétentes d'un pays tiers où se trouve le fournisseur de services auquel il est demandé de fournir des données en cas de conflit de lois afin d'éviter des interprétations subjectives de la part d'un tribunal unique.
16) La validité et la durée des injonctions de conservation devraient être davantage liées aux injonctions de production qui les accompagnent.
17) La sécurité des transferts de données devrait être mieux garantie.
18) La vérification de l'authenticité des données devrait être prévue, en particulier lorsque des données cryptées pourraient être fournies.

Le Comité européen de la protection des données

La présidente

(Andrea Jelinek)