

# CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

## **Résumé de l'avis du Contrôleur européen de la protection des données sur les propositions relatives aux injonctions européennes de production et conservation de preuves électroniques en matière pénale**

*(Le texte complet de cet avis est disponible en allemand, en anglais et en français sur le site internet du CEPD: [www.edps.europa.eu](http://www.edps.europa.eu))*

(2020/C 32/04)

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.

## 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 <sup>(1)</sup>, dont:
  - une proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale <sup>(2)</sup> (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 <sup>(3)</sup> (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») <sup>(4)</sup>, 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 <sup>(5)</sup>. Tous les États membres qui ont participé à l'adoption de la directive DEE <sup>(6)</sup> avaient jusqu'en mai 2017 pour la transposer dans leur législation nationale <sup>(7)</sup>.
3. Le 26 septembre 2018, le comité européen de la protection des données <sup>(8)</sup> (ci-après le «comité») a adopté un avis <sup>(9)</sup> 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 <sup>(10)</sup> et la proposition de directive <sup>(11)</sup> 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 <sup>(12)</sup> 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 n° 185) (ci-après la «convention sur la cybercriminalité») <sup>(13)</sup>. Les deux recommandations ont fait l'objet de deux avis du CEPD <sup>(14)</sup>. 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») <sup>(15)</sup>, 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 <sup>(16)</sup>.
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 <sup>(17)</sup>. 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.

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.

## 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*

(<sup>1</sup>) 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>

(<sup>2</sup>) 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.

- (<sup>3</sup>) 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.
- (<sup>4</sup>) 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).
- (<sup>5</sup>) 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].
- (<sup>6</sup>) Tous les États membres de l'Union, à l'exception du Danemark et de l'Irlande.
- (<sup>7</sup>) 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](https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120)
- (<sup>8</sup>) 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.
- (<sup>9</sup>) 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](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2018-09-26-eevidence_fr.pdf)
- (<sup>10</sup>) <https://www.consilium.europa.eu/fr/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/#>
- (<sup>11</sup>) <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/>
- (<sup>12</sup>) 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.
- (<sup>13</sup>) 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 n° 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).
- (<sup>14</sup>) 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.
- (<sup>15</sup>) Disponible à l'adresse suivante: <https://www.congress.gov/bill/115th-congress/house-bill/1625/text>
- (<sup>16</sup>) [https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act\\_fr](https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_fr)
- (<sup>17</sup>) <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-counteracting-serious-crime-cs-usa-no62019>
-