

Bruxelles, le 30 novembre 2018  
(OR. en)

15020/18

---

---

**Dossier interinstitutionnel:  
2018/0108(COD)**

---

---

JAI 1236  
COPEN 428  
CYBER 304  
DROIPEN 192  
JAIEX 160  
ENFOPOL 596  
DAPIX 366  
EJUSTICE 163  
MI 917  
TELECOM 442  
DATAPROTECT 263  
CODEC 2180

#### NOTE

---

Origine:	la présidence
Destinataire:	Conseil
N° doc. préc.:	14351/1/18 REV1
N° doc. Cion:	8110/18
Objet:	Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale - Orientation générale

---

#### INTRODUCTION

1. Le 17 avril 2018, la Commission a adopté et transmis au Conseil et au Parlement européen la proposition visée en objet, dont la base juridique est l'article 82, paragraphe 1, du TFUE. La proposition crée une injonction européenne de production et une injonction européenne de conservation en vue d'obtenir et de conserver des preuves électroniques dans une autre juridiction sans intervention des autorités compétentes de cette juridiction. Les injonctions visent spécifiquement l'accès transfrontière aux preuves électroniques dans le but d'adapter les mécanismes de coopération judiciaire aux exigences de la lutte contre la criminalité à l'ère numérique.

2. Le règlement proposé prévoit la possibilité de demander toute catégorie de données stockées. Il fixe toutefois un seuil spécifique pour les données relatives aux transactions et au contenu [par opposition aux données relatives aux abonnés et à l'accès], qui ne peuvent être demandées que pour les infractions pénales passibles dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans ou pour les infractions purement informatiques, relevant de la cybercriminalité ou liées au terrorisme.
3. La proposition envisage de fixer à 10 jours le délai obligatoire pour mettre en œuvre l'injonction européenne de production mais, dans des situations d'urgence (menace imminente pour la vie ou l'intégrité physique d'une personne ou pour une infrastructure critique), le délai est ramené à 6 heures. Pour ce qui concerne l'injonction européenne de conservation, l'autorité compétente a 60 jours pour confirmer qu'elle a introduit une demande ultérieure de production des données (y compris au moyen de l'entraide judiciaire). En cas de non-conformité à une injonction, des sanctions peuvent être imposées au fournisseur de services.
4. Les injonctions doivent être adressées à un fournisseur de services proposant des services dans l'Union ou à un représentant légal qui se trouve dans un autre État membre et qui est désigné par le fournisseur de services aux fins de recueillir des preuves électroniques conformément à une proposition de directive établissant les règles harmonisées en la matière. Le règlement proposé utilise comme critères les types de services proposés (services de communications électroniques, de la société de l'information, d'hébergement, de numérotation IP, d'anonymisation et d'enregistrement fiduciaire) et cite certains types de fournisseurs de services (bureaux d'enregistrement et registres de noms de domaine).
5. Le 18 octobre 2018, le Conseil européen<sup>1</sup> a demandé qu'une solution soit trouvée pour assurer un accès transfrontière rapide et effectif aux preuves numériques afin de lutter efficacement contre le terrorisme et d'autres formes de grande criminalité organisée, tant au sein de l'UE qu'au niveau international. Il a souligné qu'il convenait, d'ici la fin de la législature, de parvenir à un accord concernant les propositions de la Commission.
6. Au Parlement européen, M<sup>me</sup> Birgit Sippel (LIBE, S&D) a été nommée rapporteure le 24 mai 2018. La commission LIBE a examiné la proposition le 11 juin 2018 et a tenu plusieurs réunions et auditions, dont une audition publique le 27 novembre 2018. Aucun calendrier n'a été fixé pour l'adoption du rapport.
7. Le Comité économique et social européen a adopté son avis le 12 juillet 2018<sup>2</sup>.

---

<sup>1</sup> EUCO 13/18, point 9.

<sup>2</sup> 11533/18.

## II. TRAVAUX AU SEIN DU CONSEIL

8. La Commission a présenté sa proposition au groupe COPEN le 27 avril 2018. Le groupe a ensuite procédé à un examen article par article et à un échange de vues sur l'analyse d'impact les 5 et 6 mai 2018. D'une manière générale, tant l'analyse d'impact que la proposition ont reçu un accueil favorable de la part des délégations.
9. Les travaux ont principalement porté sur la suggestion de la Commission consistant à signifier ou notifier une injonction européenne de production directement au fournisseur de services ou à son représentant légal, sans intervention de l'État membre dans lequel celui-ci se trouve (c'est-à-dire l'État chargé de la mise en œuvre), sur la définition de fournisseur de services, les immunités et privilèges, la procédure de réexamen en cas d'obligations contradictoires, ainsi que sur les sanctions pour non-conformité avec les obligations au titre du règlement.
10. Le groupe a examiné la proposition sous les présidences bulgare et autrichienne. Douze réunions ont été tenues, qui ont donné lieu à cinq versions révisées consécutives. Les discussions ont été clôturées le 20 novembre 2018 dans le but de présenter le texte de compromis figurant à l'annexe de la présente note au Conseil JAI des 6 et 7 décembre 2018, pour adoption d'une orientation générale.
11. Les résultats des discussions lors des réunions du groupe, les contributions écrites reçues des délégations ainsi que les réserves émises par les États membres à propos du texte ont été pris en compte dans le texte de compromis révisé établi par la présidence qui figure en annexe. Les considérants ont été adaptés pour tenir compte des modifications apportées au dispositif. Toutes les modifications par rapport à la proposition de la Commission sont signalées par des **caractères gras** (passages nouveaux) ou des crochets [...] (suppressions).

### III. CONCLUSION

12. Le texte tel qu'il figure en annexe traduit les efforts déployés par la présidence et les États membres pour parvenir à un compromis.
  13. Le 28 novembre 2018, le Comité des représentants permanents est parvenu à un accord sur le texte de compromis de la présidence tel qu'il figure à l'annexe de la présente note, avec une seule modification concernant la levée de la réserve émise dans la Slovénie (note de bas de page n° 27).
  14. Au vu de ce qui précède, le Conseil est invité à dégager une orientation générale sur ce texte, laquelle servira ensuite de base aux négociations qui seront menées avec le Parlement européen dans le cadre de la procédure législative ordinaire (article 294 du TFUE).
-

Proposition de

**RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale<sup>3</sup>**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen<sup>4</sup>,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

- (1) L'Union s'est donné pour objectif de maintenir et de développer un espace de liberté, de sécurité et de justice. En vue de l'établissement progressif de cet espace, l'Union doit adopter des mesures relevant du domaine de la coopération judiciaire en matière pénale fondée sur le principe de reconnaissance mutuelle des jugements et des décisions judiciaires, principe communément considéré comme la pierre angulaire de la coopération judiciaire en matière pénale dans l'Union depuis le Conseil européen de Tampere des 15 et 16 octobre 1999.
- (2) Les mesures visant à obtenir et à conserver des preuves électroniques sont de plus en plus importantes pour permettre des enquêtes et des poursuites pénales dans l'ensemble de l'Union. Des mécanismes efficaces pour obtenir des preuves électroniques sont essentiels pour lutter contre la criminalité, sous réserve de conditions garantissant le plein respect des droits et principes fondamentaux reconnus dans la charte des droits fondamentaux de l'Union européenne tels que consacrés dans les traités, et en particulier les principes de nécessité et de proportionnalité, de légalité, de protection des données, de secret de la correspondance et de protection de la vie privée.

---

<sup>3</sup> Les Pays-Bas, la Finlande, la République tchèque et la Lettonie ont émis une réserve sur l'ensemble du texte. Pour ce qui est des Pays-Bas, cette réserve porte entre autres sur les articles 5, 6 et 7 *bis*, l'article 11, paragraphe 1, et les articles 12 *bis*, 12 *ter*, 14 et 17.

<sup>4</sup> JO C du, p. .

- (3) La déclaration conjointe des ministres de la justice et des affaires intérieures du 22 mars 2016 et des représentants des institutions de l'Union sur les attentats terroristes à Bruxelles a souligné la nécessité de trouver en priorité des moyens de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement et de définir des mesures concrètes pour s'attaquer à cette question.
- (4) Les conclusions du Conseil du 9 juin 2016 ont souligné l'importance croissante des preuves électroniques dans les procédures pénales, et de protéger le cyberspace contre les abus et les activités criminelles au profit des économies et des sociétés, et donc la nécessité pour les autorités répressives et judiciaires de disposer d'outils efficaces pour enquêter sur les actes délictueux commis en rapport avec le cyberspace et en poursuivre les auteurs.
- (5) Dans la communication conjointe sur la résilience, la dissuasion et la défense du 13 septembre 2017<sup>5</sup>, la Commission a souligné que l'efficacité des enquêtes et des poursuites relatives aux infractions facilitées par les technologies de l'information et de la communication constitue un moyen de dissuasion essentiel contre les cyberattaques, et que le cadre procédural actuel doit être mieux adapté à l'ère d'internet. Les procédures actuelles ne sont pas toujours suffisantes en raison de la rapidité des cyberattaques, qui créent un besoin particulier de coopération transfrontière rapide.
- (6) Le Parlement européen a repris ces préoccupations dans sa résolution sur la lutte contre la cybercriminalité du 3 octobre 2017<sup>6</sup>, en soulignant les défis que le cadre juridique actuellement fragmenté peut créer pour les fournisseurs de services cherchant à se conformer aux demandes des services répressifs, et en appelant la Commission à élaborer un cadre juridique pour les preuves électroniques offrant des garanties suffisantes pour les droits et les libertés de tous les intéressés.
- (7) Les services basés sur un réseau peuvent être fournis à partir de n'importe quel endroit et ne nécessitent pas d'infrastructure physique, de locaux ou de personnel dans le pays concerné. En conséquence, les éléments de preuve pertinents sont souvent stockés hors de l'État menant l'enquête ou par un fournisseur de services établi en dehors de cet État. Il n'existe souvent pas d'autre lien entre l'affaire faisant l'objet de l'enquête dans l'État concerné et l'État du lieu de stockage ou de l'établissement principal du fournisseur de services.
- (8) En raison de ce manque de lien, des demandes de coopération judiciaire sont souvent adressées à des États qui hébergent un grand nombre de fournisseurs de services, mais qui n'ont aucun autre rapport avec le cas en question. En outre, le nombre de demandes s'est multiplié en raison de l'utilisation croissante des services en réseau, qui sont transfrontières par nature. En conséquence, l'obtention de preuves électroniques par les canaux de coopération judiciaire prend souvent beaucoup de temps, un délai plus long que celui de la disponibilité des indices. Il n'existe par ailleurs pas de cadre clair pour la coopération avec les fournisseurs de services, tandis que certains fournisseurs de pays tiers acceptent des demandes directes de données non relatives au contenu, conformément à leur législation nationale applicable. En conséquence, tous les États membres s'appuient sur le canal de coopération avec les fournisseurs de services lorsqu'il existe, en utilisant différents outils nationaux et différentes conditions et procédures nationales. En outre, pour les données relatives au contenu, certains États membres ont pris des mesures unilatérales, tandis que d'autres continuent de s'appuyer sur la coopération judiciaire.

---

<sup>5</sup> JOIN(2017) 450 final.

<sup>6</sup> 2017/2068(INI).

- (9) La fragmentation du cadre juridique crée des défis pour les fournisseurs de services qui cherchent à se conformer aux demandes des services répressifs. Par conséquent, il est nécessaire de proposer un cadre juridique européen pour les preuves électroniques afin d'imposer aux fournisseurs de services entrant dans le champ d'application de l'instrument l'obligation de répondre directement aux autorités sans l'intervention **systematique** [...] d'une autorité judiciaire de l'État membre du fournisseur de services **dans chaque cas**.
- (10) Les injonctions au titre du présent règlement doivent être adressées aux représentants légaux des fournisseurs de services désignés à cet effet. Si un fournisseur de services établi dans l'Union n'a pas désigné de représentant légal, les injonctions peuvent être adressées à tout établissement de ce fournisseur de services dans l'Union. Cette option de repli sert à garantir l'efficacité du système si le fournisseur de services n'a pas (encore) désigné de représentant spécifique.
- (11) Le mécanisme des injonctions européennes de production et de conservation de preuves électroniques en matière pénale ne peut fonctionner que sur la base d'un niveau élevé de confiance mutuelle entre les États membres, qui constitue une condition préalable essentielle au bon fonctionnement de cet instrument.
- (12) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus en particulier par la charte des droits fondamentaux de l'Union européenne. Ceux-ci comprennent le droit à la liberté et à la sécurité, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif et à un procès équitable, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité, ainsi que le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction.
- (12 bis) Si l'État d'émission dispose d'éléments indiquant qu'une procédure pénale parallèle pourrait être en cours dans un autre État membre, il consulte les autorités de cet État membre conformément à la décision-cadre 2009/948/JAI du Conseil<sup>7</sup>. En tout état de cause, une injonction européenne de production ne devrait pas être émise si l'État d'émission dispose d'éléments indiquant que ce serait contraire au principe *non bis in idem*.**

---

<sup>7</sup> [Décision-cadre 2009/948/JAI du Conseil](#) du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales (JO L 328 du 15.12.2009, p. 42).

- (13) Afin de garantir le plein respect des droits fondamentaux, le présent règlement se réfère explicitement aux normes nécessaires concernant l'obtention de toutes données à caractère personnel, le traitement de ces données, le contrôle juridictionnel du recours à la mesure d'enquête prévue par le présent instrument et les recours disponibles.
- (14) Le présent règlement s'applique sans préjudice des droits procéduraux dans les procédures pénales énoncés dans les directives 2010/64/UE<sup>8</sup>, 2012/13/UE<sup>9</sup>, 2013/48/UE<sup>10</sup>, 2016/343<sup>11</sup>, 2016/800<sup>12</sup> et 2016/1919<sup>13</sup> du Parlement européen et du Conseil.
- (15) Le présent instrument fixe les règles selon lesquelles une autorité judiciaire compétente de l'Union européenne peut ordonner à un fournisseur de services proposant des services dans l'Union de produire ou de conserver des preuves électroniques au moyen d'une injonction européenne de production ou de conservation. Le présent règlement s'applique dans tous les cas où le fournisseur de services est établi ou représenté dans un autre État membre. Dans le contexte national où les instruments prévus par le présent règlement ne peuvent être utilisés, le règlement ne doit pas limiter pas les pouvoirs des autorités nationales compétentes déjà prévus par la législation nationale pour contraindre les fournisseurs de services établis ou représentés sur leur territoire.

---

<sup>8</sup> [Directive 2010/64/UE](#) du Parlement européen et du Conseil du 20 octobre 2010 relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales (JO L 280 du 26.10.2010, p. 1).

<sup>9</sup> [Directive 2012/13/UE](#) du Parlement européen et du Conseil du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales (JO L 142 du 1.6.2012, p. 1).

<sup>10</sup> [Directive 2013/48/UE](#) du Parlement européen et du Conseil du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires (JO L 294 du 6.11.2013, p. 1).

<sup>11</sup> [Directive \(UE\) 2016/343](#) du Parlement européen et du Conseil du 9 mars 2016 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales (JO L 65 du 11.3.2016, p. 1).

<sup>12</sup> [Directive \(UE\) 2016/800](#) du Parlement européen et du Conseil du 11 mai 2016 relative à la mise en place de garanties procédurales en faveur des enfants qui sont des suspects ou des personnes poursuivies dans le cadre des procédures pénales (JO L 132 du 21.5.2016, p. 1).

<sup>13</sup> [Directive \(UE\) 2016/1919](#) du Parlement européen et du Conseil du 26 octobre 2016 concernant l'aide juridictionnelle pour les suspects et les personnes poursuivies dans le cadre des procédures pénales et pour les personnes dont la remise est demandée dans le cadre des procédures relatives au mandat d'arrêt européen (JO L 297 du 4.11.2016, p. 1).



- (16) Les fournisseurs de services les plus pertinents pour les procédures pénales sont les fournisseurs de services de communications électroniques et les fournisseurs spécifiques de services de la société de l'information qui facilitent les interactions entre les utilisateurs. Dès lors, ces deux groupes sont couverts par le présent règlement. Les fournisseurs de services de communications électroniques sont définis dans la proposition de directive établissant le code des communications électroniques européen. Ils comprennent les communications interpersonnelles telles que la voix par le protocole de l'internet, la messagerie instantanée et les services de courrier électronique. **Le présent règlement devrait aussi s'appliquer à d'autres [...] fournisseurs de services de la société de l'information au sens de la directive (UE) 2015/1535 [...] qui ne sont pas considérés comme des fournisseurs de services de communications électroniques [...] mais qui offrent à leurs utilisateurs la possibilité de communiquer les uns avec les autres ou leur proposent des services qui peuvent être utilisés pour traiter ou stocker des données pour leur compte, ce qui correspond aux termes utilisés dans la convention de Budapest sur la cybercriminalité. Le traitement des données devrait être compris au sens technique de création ou modification de données, c'est-à-dire des opérations techniques destinées à produire ou modifier des données en faisant appel à de la puissance de calcul. Les catégories de fournisseurs de services visées ici sont, par exemple, les places de marché en ligne [...] offrant aux consommateurs [...] et aux entreprises la possibilité de communiquer les uns avec les autres et les autres services d'hébergement, notamment lorsque le service est fourni par l'intermédiaire de l'informatique en nuage, ainsi que les plateformes de jeux en ligne et les plateformes de jeux d'argent et de hasard en ligne. Lorsqu'un fournisseur de services de la société de l'information n'offre pas à ses utilisateurs la possibilité de communiquer les uns avec les autres mais uniquement de communiquer avec le fournisseur de services ou n'offre pas la possibilité de traiter ou stocker des données ou que la possibilité de stocker/traiter des données ne constitue pas une partie essentielle du service fourni aux utilisateurs, tels que les services juridiques ou les services d'architecture, d'ingénierie et de comptabilité fournis à distance en ligne, il n'entrerait pas dans le champ d'application du présent règlement, même s'il relève de la définition des services de la société de l'information conformément à la directive (UE) 2015/1535. [...]**
- (17) Dans de nombreux cas, les données ne sont plus stockées ou traitées sur le dispositif d'un utilisateur, mais rendues disponibles sur une infrastructure en nuage pour un accès à partir de n'importe quel endroit. Pour opérer ces services, les fournisseurs de services n'ont pas besoin d'être établis ou d'avoir des serveurs sur un territoire spécifique. Ainsi, l'application du présent règlement ne peut dépendre de la localisation réelle de l'établissement du fournisseur ou de l'installation de traitement ou de stockage des données.
- (18) Les fournisseurs de services d'infrastructure internet liés à l'attribution de noms et de numéros, tels que les bureaux d'enregistrement et les registres de noms de domaine et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, ou les registres internet régionaux pour les adresses de protocole internet (IP), sont particulièrement pertinents lorsqu'il s'agit d'identifier des acteurs cachés derrière des sites internet malveillants ou compromis. Ils détiennent des données particulièrement pertinentes pour les procédures pénales, qui permettent d'identifier une personne ou une entité cachée derrière un site internet utilisé dans une activité criminelle, ou la victime d'une activité criminelle si un site internet compromis a été détourné par des criminels.

- (19) Le présent règlement régit la collecte des données stockées uniquement, c'est-à-dire des données détenues par un fournisseur de services au moment de la réception d'un certificat d'injonction européenne de production ou de conservation. Il ne prévoit pas d'obligation générale de conservation des données, et n'autorise pas l'interception de données ou l'obtention de données stockées à un moment ultérieur à la réception d'un certificat d'injonction de production ou de conservation. Les données doivent être fournies, qu'elles soient cryptées ou non.
- (20) 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.
- (21) Il y a donc lieu de distinguer les données relatives à l'accès comme une catégorie de données spécifique utilisée dans le présent règlement. Les données relatives à l'accès sont demandées pour le même objectif que les données relatives aux abonnés, à savoir pour identifier l'utilisateur sous-jacent, et le niveau d'interférence avec les droits fondamentaux est similaire à celui des données relatives aux abonnés. Les données relatives à l'accès sont généralement enregistrées dans le cadre d'un enregistrement d'événements (un journal de serveur) pour indiquer le début et la fin d'une session d'accès d'un utilisateur à un service. Il s'agit souvent d'une adresse IP individuelle (statique ou dynamique) ou d'un autre identifiant qui indique l'interface réseau utilisée lors de la session d'accès. Si l'utilisateur est inconnu, il est souvent nécessaire de l'identifier avant que les données relatives aux abonnés liées à cet identifiant puissent être demandées au fournisseur de services.
- (22) D'autre part, les données relatives aux transactions sont généralement demandées pour obtenir des informations sur les contacts de l'utilisateur et le lieu où il se trouve, et peuvent servir à établir le profil d'une personne concernée. Cela dit, les données relatives à l'accès seules ne peuvent pas servir à atteindre un objectif similaire; car elles ne révèlent par exemple aucune information sur les interlocuteurs de l'utilisateur. Dès lors, la présente proposition introduit une nouvelle catégorie de données, qui doivent être traitées comme des données relatives aux abonnés si l'objectif de la demande d'obtention de ces données est similaire.
- (23) Toutes les catégories de données contiennent des données à caractère personnel et sont par conséquent couvertes par les garanties prévues par l'acquis de l'Union en matière de protection des données, mais l'intensité de l'incidence sur les droits fondamentaux varie, en particulier entre les données relatives aux abonnés et les données relatives à l'accès d'une part et les données relatives aux transactions et les données relatives au contenu d'autre part. Alors que les données relatives aux abonnés et les données relatives à l'accès sont utiles pour obtenir de premiers indices dans une enquête sur l'identité d'un suspect, les données relatives aux transactions et les données relatives au contenu sont les plus pertinentes en tant que matériel probant. Il est donc essentiel que toutes ces catégories de données soient couvertes par l'instrument. En raison du degré d'interférence différent avec les droits fondamentaux, des conditions différentes sont imposées pour obtenir des données relatives aux abonnés et des données relatives à l'accès, d'une part, et des données relatives aux transactions et des données relatives au contenu, d'autre part.

- (24) L'injonction européenne de production et l'injonction européenne de conservation sont des mesures d'enquête qui ne doivent être prises que dans le cadre de procédures pénales spécifiques contre les auteurs connus ou encore inconnus d'une infraction pénale concrète qui a déjà été commise, après une évaluation individuelle de la proportionnalité et de la nécessité dans chaque cas.
- (24 bis) Les procédures en matière d'entraide judiciaire pouvant être considérées comme des procédures pénales conformément à la législation nationale applicable dans les États membres, il y a lieu de préciser qu'une injonction européenne de production ne devrait pas être émise pour fournir une entraide judiciaire à un autre État membre ou à un pays tiers. Dans ce cas, la demande d'entraide judiciaire devrait être adressée à l'État membre ou au pays tiers qui peut assurer une entraide judiciaire en vertu de sa législation nationale. Cependant, si des preuves électroniques avaient déjà été obtenues au titre du présent règlement par l'autorité d'émission aux fins de ses propres enquêtes ou procédures pénales et si, par la suite, ces preuves font l'objet d'un transfert ou d'une transmission, les conditions liées au principe de spécialité devraient s'appliquer.**
- (24 ter) Le présent règlement devrait s'appliquer aux procédures pénales engagées par l'autorité d'émission en vue de localiser une personne condamnée qui s'est soustraite à la justice afin d'exécuter une peine ou mesure de sûreté privatives de liberté. Cependant, au cas où la peine ou mesure de sûreté privatives de liberté a été prononcée par défaut, il ne devrait pas être possible d'émettre une injonction européenne de production ou une injonction européenne de conservation étant donné que la législation nationale des États membres sur les jugements par défaut varie considérablement au sein de l'Union européenne.**
- (25) Le présent règlement est sans préjudice des pouvoirs d'enquête des autorités dans les procédures civiles ou administratives, notamment lorsque ces procédures peuvent entraîner des sanctions.
- (26) Le présent règlement s'applique aux fournisseurs de services qui proposent des services dans l'Union, et les injonctions prévues par le présent règlement ne peuvent être émises que pour les données relatives aux services offerts dans l'Union. Les services fournis exclusivement en dehors de l'Union n'entrent pas dans le champ d'application du présent règlement, même si le fournisseur de services est établi dans l'Union.

- (27) Pour déterminer si un fournisseur de services fournit des services dans l'Union, il est nécessaire d'évaluer si le fournisseur de services permet à des personnes morales ou physiques d'un ou plusieurs États membres d'utiliser ses services. Toutefois, la seule accessibilité d'une interface en ligne, comme par exemple l'accessibilité du site internet du fournisseur de services, d'un intermédiaire ou d'une adresse électronique et d'autres coordonnées dans un ou plusieurs États membres prises isolément ne constituent pas une condition suffisante pour l'application du présent règlement.
- (28) Un lien substantiel avec l'Union doit également être pertinent pour déterminer le champ d'application du présent règlement. Un tel lien substantiel avec l'Union doit être considéré comme existant lorsque le fournisseur de services possède un établissement dans l'Union. En l'absence d'un tel établissement, le critère de lien substantiel devrait être [...] basé [...] **sur des critères factuels spécifiques tels qu'un nombre significatif d'utilisateurs dans un ou plusieurs États membres, ou sur le ciblage des activités vers un ou plusieurs États membres.** Le ciblage des activités vers un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet État membre ou ces États membres, ou la possibilité de commander des biens ou des services. Le ciblage des activités vers un État membre peut également être constaté sur la base de la disponibilité d'une application dans la boutique d'applications nationale correspondante, de la mise à disposition de publicité locale ou de publicité dans la langue utilisée dans cet État membre ou de la gestion des relations avec la clientèle, si un service après-vente est par exemple fourni dans la langue généralement utilisée dans cet État membre. Un lien substantiel doit également être constaté lorsqu'un fournisseur de services dirige ses activités vers un ou plusieurs États membres comme énoncé à l'article 17, paragraphe 1, point c), du règlement (UE) n° 1215/2012 relatif à la compétence, à la reconnaissance et à l'exécution des décisions en matière civile et commerciale<sup>14</sup>. En revanche, la fourniture du service en vue du seul respect de l'interdiction de discrimination prévue par le règlement (UE) 2018/302<sup>15</sup> ne peut être considérée, pour ce seul motif, comme dirigeant ou ciblant des activités vers un territoire donné au sein de l'Union.
- (29) Une injonction européenne de production ne doit être émise que si elle s'avère nécessaire et proportionnée. L'évaluation devrait tenir compte du fait que l'injonction est limitée à ce qui est nécessaire pour atteindre l'objectif légitime d'obtenir les données pertinentes et nécessaires pour servir de preuve uniquement dans le cas d'espèce, **compte dûment tenu de l'incidence de la mesure sur les droits fondamentaux de la personne dont les données sont requises.**

---

<sup>14</sup> [Règlement \(UE\) n° 1215/2012](#) du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (JO L 351 du 20.12.2012, p. 1).

<sup>15</sup> [Règlement \(UE\) 2018/302](#) du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE (JO L 601 du 2.3.2018, p. 1).

- (30) Lorsqu'une injonction européenne de production ou de conservation est émise, une autorité judiciaire doit toujours être incluse dans le processus de délivrance ou de validation de l'injonction. Compte tenu du caractère plus sensible des données relatives aux transactions et des données relatives au contenu, l'émission ou la validation des injonctions européennes de production pour ces catégories nécessite le réexamen d'un juge. Les données relatives aux abonnés et à l'accès étant moins sensibles, les injonctions européennes de production pour leur divulgation peuvent également être émises ou validées par des procureurs compétents.
- (31) Pour la même raison, une distinction doit être faite en ce qui concerne le champ d'application matériel du présent règlement: les injonctions de production de données relatives aux abonnés et de données relatives à l'accès peuvent être émises pour toute infraction pénale, tandis que l'accès aux données relatives aux transactions et aux données relatives au contenu doit être soumis à des exigences plus strictes, pour refléter la nature plus sensible de ces données. Un seuil permet une approche plus proportionnée, en combinaison avec à un certain nombre d'autres conditions et garanties ex ante et ex post prévues dans la proposition pour assurer le respect de la proportionnalité et des droits des personnes concernées. En même temps, un seuil ne devrait pas limiter l'efficacité de l'instrument ni son utilisation par les praticiens. Autoriser la délivrance de décisions d'enquêtes pour des infractions assorties d'une peine d'emprisonnement d'une durée maximale d'au moins trois ans limite le champ d'application de l'instrument à des délits plus graves, sans affecter de façon excessive ses possibilités d'utilisation par les praticiens. Cela exclut du champ d'application un nombre significatif de délits considérés comme moins graves par les États membres, qui donnent lieu à une peine maximale plus courte. Cela offre également l'avantage d'être plus facile à appliquer dans la pratique.
- (32) Il existe des infractions spécifiques pour lesquelles les preuves sont généralement disponibles exclusivement sous forme électronique, par nature particulièrement éphémère. C'est le cas des infractions relevant de la cybercriminalité, même celles qui ne sont pas forcément considérées comme graves en tant que telles mais qui peuvent causer des préjudices graves ou considérables, en particulier dans le cas où le préjudice individuel est faible mais touche globalement un grand nombre de victimes. Dans la plupart des cas où l'infraction a été commise au moyen d'un système d'information, l'application du même seuil que pour d'autres types d'infractions conduirait généralement à l'impunité. Cela justifie que le règlement s'applique également aux infractions pour lesquelles la sanction est inférieure à trois ans d'emprisonnement. Les infractions supplémentaires liées au terrorisme telles que décrites dans la directive 2017/541/UE ne requièrent pas de seuil relatif à une durée maximale d'emprisonnement d'au moins trois ans.
- (33) En outre, il est nécessaire de prévoir que l'injonction européenne de production ne peut être émise que si une mesure similaire est disponible pour la même infraction dans une situation nationale comparable dans l'État d'émission.
- (33 bis) Dans les cas où une injonction est émise en vue d'obtenir différentes catégories de données, l'autorité d'émission doit veiller à ce que les conditions et procédures, par exemple la notification à l'État chargé de la mise en œuvre, soient respectées pour toutes les catégories de données concernées.**

(34) Dans les cas où les données demandées sont stockées ou traitées dans le cadre d'une infrastructure mise à disposition par un fournisseur de services à une entreprise ou à une autre entité que des personnes physiques, généralement dans le cas de services d'hébergement, l'injonction européenne de production ne doit être utilisée que lorsque d'autres mesures d'enquêtes visant l'entreprise ou l'entité ne sont pas appropriées, surtout si cela risque de compromettre l'enquête. Ceci est particulièrement pertinent lorsqu'il s'agit de grandes entités, telles que des grandes entreprises ou des administrations publiques, qui utilisent elles-mêmes les services de fournisseurs de services pour fournir leur infrastructure informatique ou leurs services informatiques institutionnels, ou les deux. Le premier destinataire d'une injonction européenne de production, dans de telles situations, doit être l'entreprise ou l'autre entité. Cette entreprise ou cette autre entité ne peut pas être un fournisseur de services couvert par le champ d'application du présent règlement. Toutefois, pour les cas où l'application à cette entité n'est pas opportune, par exemple parce que l'entité est soupçonnée d'être impliquée dans l'affaire en question ou s'il existe des indices de collusion avec la cible de l'enquête, les autorités compétentes doivent pouvoir s'adresser au fournisseur de services concerné pour fournir les données demandées. Cette disposition n'affecte pas le droit de demander au fournisseur de services de conserver les données.

**(34 bis) Au cas où les données sont stockées ou traitées dans le cadre d'une infrastructure fournie par un fournisseur de services à une autorité publique, seules les autorités du même État membre devraient être en mesure d'émettre une injonction européenne de production ou une injonction européenne de conservation parce que de telles données peuvent être considérées comme particulièrement sensibles. La notion d'autorité publique devrait être comprise au sens d'une autorité habilitée par le droit national applicable à régir ou administrer certaines parties ou certains aspects de la vie publique, par exemple des autorités relevant du pouvoir exécutif, législatif ou judiciaire au niveau de l'État, d'une province ou d'une municipalité.**

(35) Les immunités et les privilèges, qui peuvent concerner des catégories de personnes (comme les diplomates) ou des relations spécifiquement protégées (comme le privilège des confidences à l'avocat **ou le droit des journalistes de ne pas divulguer leurs sources**), sont mentionnés dans d'autres instruments de reconnaissance mutuelle comme la décision d'enquête européenne. Leur portée et leur incidence diffèrent selon la législation nationale applicable qui doit être prise en considération au moment de l'émission de l'injonction, étant donné que l'autorité d'émission ne peut émettre l'injonction que si une injonction similaire est disponible dans une situation nationale comparable. [...] **La question de savoir s'il y a lieu de tenir compte d'un deuxième cadre juridique devrait dépendre de la force du lien de la personne dont les données sont requises avec l'État d'émission. Lorsque la personne réside sur le territoire de l'État d'émission, il existe un lien fort avec cet État. Par conséquent, le cadre juridique applicable pour évaluer les immunités et privilèges devrait être exclusivement celui de l'État d'émission. Le même principe vaut pour les règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias et pour les intérêts fondamentaux de l'État chargé de la mise en œuvre. Au moment où une demande de données relatives aux transactions ou de données relatives au contenu est introduite, les autorités disposeront généralement d'éléments indiquant où la personne réside, issus de mesures d'enquête antérieures. Par ailleurs, les statistiques montrent que, dans la grande majorité des cas, la personne réside dans l'État d'émission. Lorsque tel n'est pas le cas, par exemple parce que la personne dont les données sont requises a pris des dispositions pour dissimuler où elle se trouve, le même principe devrait s'appliquer.**

**(35 bis)** Les immunités et privilèges ainsi que les règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, qui protègent [...] les données relatives aux transactions ou les données relatives au contenu dans l'État [...] chargé de la mise en œuvre [...] devraient donc être prises en considération [...] lorsque l'autorité d'émission est fondée à croire que la personne dont les données sont requises ne réside pas sur son territoire. [...] Ceci est particulièrement pertinent si la législation de [...] cet État membre [...] prévoit une protection plus élevée que la législation de l'État d'émission. La disposition garantit également le respect des cas où la divulgation des données peut porter atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales. [...] Ces aspects devraient être pris en considération non seulement lors de l'émission de l'injonction, mais également plus tard, [...] et si une procédure de mise en œuvre est engagée par l'autorité chargée de la mise en œuvre.

**(35 ter)** Lorsque l'autorité d'émission cherche à obtenir des données relatives aux transactions et est fondée à croire que la personne dont les données sont requises ne réside pas sur son territoire et que les données requises sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État chargé de la mise en œuvre ou par des règles de cet État membre sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, ou que leur divulgation peut porter atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales, l'autorité d'émission devrait demander des éclaircissements, notamment en procédant à des consultations appropriées.

**(35 quater)** Dans les cas où l'injonction européenne de production concerne des données relatives au contenu et où l'autorité d'émission est fondée à croire que la personne dont les données sont requises ne réside pas sur son territoire, l'État chargé de la mise en œuvre fait l'objet d'une notification et peut, dans les meilleurs délais et de préférence dans les dix jours, informer l'autorité d'émission des éléments qui pourraient entraîner le retrait ou l'adaptation de l'injonction, par exemple les privilèges ou immunités de la personne dont les données sont requises ou des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias. À l'inverse des données non relatives au contenu, les données relatives au contenu sont particulièrement sensibles parce que les personnes peuvent y révéler des opinions ou des détails sensibles concernant leur vie privée, ce qui justifie un traitement différent et l'intervention des autorités de l'État chargé de la mise en œuvre à un stade précoce de la procédure. Dans ces cas, l'État d'émission devrait fournir une copie du certificat à l'État chargé de la mise en œuvre au moment même où le certificat est communiqué au fournisseur de services. Dans le souci de permettre une vérification rapide, l'autorité d'émission devrait opter pour l'une des langues acceptées par l'État chargé de la mise en œuvre si une traduction du certificat est nécessaire, même lorsque le fournisseur de services a indiqué qu'il accepterait également des certificats dans une autre langue qu'une des langues officielles de l'État chargé de la mise en œuvre. Lorsque [...] l'autorité notifiée soulève des questions, elle devrait fournir à l'autorité d'émission toute information pertinente concernant les immunités ou privilèges ainsi que les règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias applicables à la personne en vertu de la législation nationale ou des informations ou si l'injonction porte atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales.

**(35 quinquies)** Dans les cas où, au moment où l'injonction européenne de production est émise, la personne a plusieurs lieux de résidence dont un est situé sur le territoire de l'État d'émission ou dans les cas où le lieu de résidence de la personne ne peut être déterminé au prix d'efforts raisonnables et proportionnés, les procédures décrites ci-dessus ne s'appliquent pas. Cependant, une brève visite, des vacances ou un séjour similaire dans l'État d'émission, sans autre lien substantiel, ne suffit pas pour qu'il y ait résidence dans cet État membre.

**(35 sexies)** Afin d'assurer une procédure rapide, le moment à prendre en compte pour déterminer s'il y a lieu d'adresser une notification aux autorités de l'État chargé de la mise en œuvre devrait être le moment où l'injonction est émise ou validée. Tout changement ultérieur de lieu de résidence ne devrait avoir aucune incidence sur la procédure. Lorsque l'autorité d'émission n'était pas fondée à croire que la personne dont les données sont requises ne réside pas sur son territoire au moment où l'injonction est émise ou validée et qu'il apparaît ultérieurement que cette personne ne résidait en fait pas sur le territoire de l'État d'émission, aucune vérification ou notification ultérieure ne devrait être requise. Cependant, la personne concernée peut, tout au long de la procédure pénale, invoquer ses droits ainsi que les règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, et l'autre État membre pourrait aussi faire valoir ses intérêts fondamentaux, tels que la sécurité et la défense nationales, à tout moment au cours de la procédure pénale. Par ailleurs, ces motifs pourraient aussi être invoqués au cours de la procédure de mise en œuvre.



**(35 septies)** Lorsque les données sont protégées par des privilèges ou immunités ou par des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias applicables en vertu de la législation de l'État chargé de la mise en œuvre ou lorsque leur divulgation pourrait porter atteinte aux intérêts fondamentaux de cet État membre, l'État d'émission devrait veiller à ce que ces motifs soient pris en considération de la même manière que s'ils avaient été prévus par sa législation nationale afin de leur donner effet. Si, par exemple, ces privilèges ou immunités ne sont pas applicables en vertu de la législation de l'État d'émission, la protection devrait, dans la mesure du possible, être adaptée aux privilèges ou immunités équivalents les plus proches en vertu de la législation de l'État d'émission, compte tenu des objectifs et des intérêts liés à la protection spécifique et des effets qui y sont attachés. Les effets juridiques prévus dans la législation nationale de l'État d'émission pour les situations similaires de ce genre devraient s'appliquer. Aux fins de déterminer comment prendre ces motifs en considération de la même manière que s'ils avaient été prévus par sa législation nationale, l'autorité d'émission peut contacter l'autorité notifiée pour obtenir de plus amples informations sur la nature et les effets de la protection, soit directement, soit par l'intermédiaire du Réseau judiciaire européen ou d'Eurojust. Si l'État chargé de la mise en œuvre peut formuler toute objection sur la base de ces motifs, la personne dont les données sont requises ne peut invoquer que ses propres droits, tels que des privilèges ou immunités, et ne peut formuler d'objections sur la base d'un intérêt fondamental de l'État chargé de la mise en œuvre.

**(35 octies)** Lorsqu'un privilège ou une immunité interdit l'utilisation des données mais que ces droits pourraient être levés et que l'autorité d'émission a l'intention d'utiliser les données obtenues comme preuve ou ne retire pas l'injonction au cas où les données n'ont pas été obtenues, l'État d'émission devrait avoir la possibilité de demander à l'autorité compétente de demander la levée du privilège ou de l'immunité.

**(36)** L'injonction européenne de conservation peut être émise pour n'importe quelle infraction. Elle vise à empêcher l'effacement, la suppression ou la modification des données concernées lorsque leur production risque de prendre plus de temps, par exemple en raison de l'utilisation de canaux de coopération judiciaire.

**(36 bis)** Afin de garantir la protection intégrale des droits fondamentaux, toute validation d'une injonction européenne de production ou d'une injonction européenne de conservation par des autorités judiciaires devrait en principe être obtenue avant l'émission de l'injonction. Il peut être dérogé à ce principe uniquement dans des cas exceptionnels et en liaison avec une demande de données relatives à l'accès et de données relatives aux abonnés, lorsque l'autorité d'émission établit de manière valable l'existence d'un cas d'urgence et qu'il n'est pas possible d'obtenir à temps la validation préalable par l'autorité judiciaire, en particulier parce qu'il n'est pas possible de joindre l'autorité de validation pour obtenir la validation et que la menace est à ce point imminente qu'une mesure immédiate doit être prise. Cependant, cette disposition s'applique uniquement si cette procédure est prévue par la législation nationale dans un cas similaire.

- (37) Les injonctions européennes de production et de conservation doivent être adressées au représentant légal désigné par le fournisseur de services. En l'absence de représentant légal désigné, les injonctions peuvent être adressées à un établissement du fournisseur de services dans l'Union. Cela peut être le cas lorsque le fournisseur de services n'a aucune obligation juridique de désigner un représentant légal. En cas de non-conformité par le représentant légal dans des situations d'urgence, l'injonction européenne de production ou de conservation peut également être adressée au fournisseur de services en complément ou en remplacement de la demande de mise en œuvre de la décision initiale conformément à l'article 14. En cas de non-conformité par le représentant légal dans des situations non urgentes, mais en cas de risques évidents de perte de données, une injonction européenne de production ou de conservation peut également être adressée à tout établissement du fournisseur de services dans l'Union. En raison de ces différents scénarios possibles, le terme général de "destinataire" est utilisé dans les dispositions. Lorsqu'une obligation telle que la confidentialité s'applique non seulement au destinataire, mais également au fournisseur de services s'il n'est pas le destinataire, cela est précisé dans la disposition correspondante. **Dans les cas où l'injonction européenne de production ou de conservation est adressée au fournisseur de services à la suite d'une non-conformité par le représentant légal, elle peut également être mise en œuvre à l'égard du fournisseur de services.**
- (38) Les injonctions européennes de production et de conservation devraient être transmises au [...] **destinataire** au moyen d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR), qui devrait être traduit. Les certificats doivent contenir les mêmes informations obligatoires que les injonctions, à l'exception des motifs de la nécessité et de la proportionnalité de la mesure ou des détails supplémentaires concernant l'affaire, afin de ne pas compromettre les enquêtes. Cependant, comme ils font partie de l'injonction elle-même, ils permettent au suspect de la contester ultérieurement au cours de la procédure pénale. Le cas échéant, le certificat doit être traduit dans la ou les langues officielles, ou dans l'une des langues officielles de [...] **l'État chargé de la mise en œuvre**, ou dans une autre langue officielle explicitement acceptée par le fournisseur de services.
- (39) L'autorité d'émission compétente **ou l'autorité compétente pour la transmission** devrait transmettre l'EPOC ou l'EPOC-PR directement au destinataire **d'une manière sécurisée et fiable** par tout moyen à même de produire une trace écrite dans des conditions permettant au fournisseur d'en établir l'authenticité, tel qu'un courrier recommandé, un courrier électronique ou des plateformes sécurisées ou d'autres canaux sécurisés, notamment ceux mis à disposition par le fournisseur de services, conformément aux règles protégeant les données à caractère personnel.
- (40) Les données requises devraient être transmises aux autorités **d'une manière sécurisée et fiable permettant d'établir l'authenticité de l'expéditeur et l'intégrité des données** au plus tard dans les 10 jours suivant la réception de l'EPOC. Des délais plus courts doivent être respectés par le fournisseur dans les cas d'urgence et si l'autorité d'émission indique d'autres raisons de s'écarter du délai de 10 jours. Outre le danger imminent de la suppression des données demandées, de telles raisons pourraient inclure des circonstances liées à une enquête en cours, par exemple lorsque les données demandées sont associées à d'autres mesures d'enquête urgentes qui ne peuvent être menées sans les données manquantes ou qui en dépendent.

- (41) Afin de permettre aux fournisseurs de services de résoudre les problèmes formels, il est nécessaire de définir une procédure pour la communication entre le fournisseur de services et l'autorité [...] d'émission dans les cas où l'EPOC serait incomplet ou contiendrait des erreurs manifestes ou des informations insuffisantes pour l'exécution de l'injonction. Par ailleurs, si le fournisseur de services ne fournit pas les informations de manière exhaustive ou en temps opportun pour toute autre raison, par exemple parce qu'il pense qu'il existe un conflit vis à vis d'une obligation soumise à la loi d'un pays tiers, ou que l'injonction européenne de production n'a pas été émise en conformité avec les conditions prévues par le présent règlement, il doit en aviser les autorités d'émission et fournir les justifications appropriées. La procédure de communication devrait donc largement permettre la correction ou le réexamen de [...] **l'injonction européenne de production** par l'autorité d'émission à un stade précoce. Pour garantir la disponibilité des données, le fournisseur de services doit conserver les données s'il peut identifier les données demandées.
- (41 bis) Le destinataire ne devrait pas être obligé de se conformer à l'injonction en cas d'impossibilité de fait que le destinataire ou, s'il ne s'agit pas de la même personne, le fournisseur de services n'a pas créée au moment de la réception de l'injonction. Il y a lieu de présumer une impossibilité de fait lorsque la personne dont les données ont été requises n'est pas un client du fournisseur de services ou ne peut pas être identifiée en tant que tel même après que des informations complémentaires aient été demandées à l'autorité d'émission, ou si les données ont été légalement supprimées avant réception de l'injonction.**
- (42) Lorsqu'il reçoit un certificat d'injonction européenne de conservation (EPOC-PR), le fournisseur de services doit conserver les données demandées pendant 60 jours au maximum, sauf si l'autorité d'émission informe le fournisseur de services qu'elle a lancé la procédure pour l'émission d'une demande ultérieure de production, auquel cas la conservation doit être poursuivie. La période de 60 jours est calculée pour permettre l'introduction d'une demande officielle. De ce fait, quelques mesures formelles au moins doivent avoir été prises, par exemple, l'envoi d'une demande d'entraide judiciaire pour la traduction. Après réception de ces informations, les données doivent être conservées aussi longtemps que nécessaire jusqu'à ce qu'elles soient produites dans le cadre d'une demande ultérieure de production.

- (43) Les fournisseurs de services et leurs représentants légaux devraient garantir la confidentialité. **Par ailleurs, ils devraient [...] s'abstenir d'informer la personne dont les données sont requises afin de protéger l'enquête sur les infractions pénales, conformément à l'article 23 du règlement (UE) 2016/679<sup>16</sup>, [...] sauf lorsque l'autorité d'émission leur demande d'informer la personne. Dans ces cas, l'autorité d'émission devrait également communiquer au fournisseur de services les informations nécessaires sur les recours légaux applicables, afin que celles-ci puissent être incluses dans les informations à la personne. En tout état de cause, l'information de l'utilisateur constitue un élément essentiel pour permettre le contrôle juridictionnel et le recours juridictionnel, et elle devrait être fournie par l'autorité s'il a été demandé au fournisseur de services de ne pas informer l'utilisateur, [...] dès lors qu'il n'y a aucun risque de compromettre les enquêtes en cours, conformément à la mesure nationale de mise en œuvre de l'article 13 de la directive (UE) 2016/680<sup>17</sup>. L'autorité d'émission peut s'abstenir d'informer la personne dont les données relatives aux abonnés et les données relatives à l'accès ont été requises si cela est nécessaire et proportionné pour protéger les droits fondamentaux et les intérêts légitimes d'une autre personne et, en particulier, lorsque ces droits et intérêts priment sur l'intérêt qu'a la personne dont les données sont requises à être informée. Tel pourrait être le cas lorsqu'une injonction porte sur les données relatives aux abonnés ou les données relatives à l'accès d'un tiers, compte tenu de la présomption d'innocence du suspect. Lorsque l'identité de la personne concernée est inconnue de l'autorité d'émission, il ne faudrait procéder à une enquête sur l'identité de cette personne que lorsque cela est nécessaire et proportionné par rapport au caractère intrusif de la mesure et à l'effort à fournir pour établir l'identité de la personne.**
- (44) En cas de non-conformité par le destinataire, l'autorité d'émission peut transférer l'injonction complète, notamment le raisonnement sur la nécessité et la proportionnalité, accompagnée du certificat, à l'autorité compétente de l'État membre où le destinataire du certificat réside ou est établi. Cet État membre doit la mettre en œuvre en conformité avec la législation nationale. Les États membres doivent prévoir l'imposition de sanctions pécuniaires efficaces, proportionnées et dissuasives en cas de violation des obligations établies par le présent règlement.

---

<sup>16</sup> [Règlement \(UE\) 2016/679](#) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

<sup>17</sup> [Directive \(UE\) 2016/680](#) du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

- (45) La procédure de mise en œuvre est une procédure par laquelle le destinataire peut [...] **invoquer des motifs formels contre** la mise en œuvre sur la base de certains motifs restreints. L'autorité chargée de la mise en œuvre peut refuser de reconnaître et de mettre en œuvre l'injonction sur la base des mêmes motifs [...] **et également, s'il y a lieu de les prendre en considération en vertu du présent règlement**, si les immunités et privilèges **ainsi que les règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias**, prévus par sa législation nationale, s'appliquent ou si la divulgation risque de porter atteinte à ses intérêts fondamentaux, tels que la sécurité et la défense nationales. L'autorité chargée de la mise en œuvre devrait consulter l'autorité d'émission avant de refuser de reconnaître ou de mettre en œuvre l'injonction sur la base de ces motifs. En cas de non-conformité, les autorités peuvent imposer des sanctions. Ces sanctions doivent être proportionnées compte tenu également des circonstances spécifiques telles que les non-conformités répétées ou systématiques.
- (45 bis) **Lorsqu'elles déterminent dans un cas d'espèce les sanctions pécuniaires appropriées, les autorités compétentes devraient tenir compte de toutes les circonstances pertinentes, telles que la nature, la gravité et la durée de l'infraction, le fait qu'elle a été commise intentionnellement ou par négligence, la question de savoir si le fournisseur de services a été tenu responsable d'infractions similaires et la solidité financière du fournisseur de services tenu responsable. Dans des circonstances exceptionnelles, cette évaluation peut amener l'autorité chargée de la mise en œuvre à s'abstenir d'imposer des sanctions pécuniaires. À cet égard, une attention particulière devrait être accordée aux micro-entreprises qui ne se conforment pas à une injonction en cas d'urgence en raison du manque de ressources humaines en dehors des heures normales de bureau, si les données sont transmises sans retard injustifié.**
- (46) [...] Les fournisseurs de services ne peuvent pas être tenus responsables dans les États membres des préjudices causés à leurs utilisateurs ou à des tiers résultant [...] de la conformité de bonne foi à un EPOC ou un EPOC-PR. **Il devrait incomber à l'autorité d'émission de garantir la légalité de l'injonction, y compris sa nécessité et sa proportionnalité.**
- (47) En plus des personnes dont les données sont demandées, les fournisseurs de services et les pays tiers peuvent être affectés par la mesure d'enquête. Par courtoisie envers les intérêts souverains des pays tiers, et afin de protéger les personnes concernées et de concilier les obligations contradictoires des fournisseurs de services, le présent instrument prévoit un mécanisme spécifique de contrôle juridictionnel si la conformité avec une injonction européenne de production empêchait les fournisseurs de services de respecter l'obligation légale découlant de la législation d'un État tiers.
- (48) À cette fin, chaque fois que le destinataire considère que dans un cas spécifique, l'injonction européenne de production entraînerait la violation d'une obligation légale découlant de la législation d'un pays tiers, il doit en informer l'autorité d'émission par l'intermédiaire d'une objection motivée en utilisant les formulaires fournis. L'autorité d'émission doit alors examiner l'injonction européenne de production à la lumière de l'objection motivée, en tenant compte des mêmes critères que ceux que la juridiction compétente devrait suivre. Lorsque l'autorité décide de maintenir l'injonction, la procédure doit être soumise à la juridiction compétente, comme notifié par l'État membre concerné, qui examine ensuite l'injonction.

- (49) Pour déterminer l'existence d'une obligation contradictoire dans les circonstances spécifiques de l'affaire examinée, la juridiction compétente [...] **peut** s'appuyer sur une expertise externe appropriée si nécessaire, par exemple [...] sur l'interprétation de la législation du pays tiers concerné. Ceci peut inclure la consultation des autorités centrales de ce pays.
- (50) Une expertise sur l'interprétation peut également être fournie par des avis d'experts lorsqu'ils sont disponibles. Les informations et la jurisprudence sur l'interprétation des législations de pays tiers et sur les procédures de résolution des conflits de lois dans les États membres doivent être mises à disposition sur une plateforme centrale telle que le projet SIRIUS et/ou le Réseau judiciaire européen. Cela devrait permettre aux tribunaux de bénéficier de l'expérience et de l'expertise acquises par d'autres tribunaux sur des questions identiques ou similaires. Cela ne devrait pas empêcher une nouvelle consultation du pays tiers le cas échéant.
- (51) Lorsque des obligations contradictoires existent, la juridiction devrait déterminer si les dispositions contradictoires **du droit** du pays tiers s'appliquent **et, si tel est le cas, si elles** interdisent la divulgation des données concernées [...]. Lorsque la juridiction conclut que des dispositions contradictoires du pays tiers interdisent la divulgation des données, [...] [...] [...] la juridiction devrait décider si elle maintient l'injonction européenne de production en prenant en considération un certain nombre d'éléments visant à déterminer la force de la connexion à l'une ou l'autre des deux juridictions concernées, les intérêts respectifs à obtenir ou à empêcher la divulgation des données, et les éventuelles conséquences pour le fournisseur de services qui devra se conformer à l'injonction.

Il est important de noter que, pour les infractions relevant de la cybercriminalité, le lieu de l'infraction désigne à la fois le ou les lieux où elle a été commise et le ou les lieux où ses effets se sont matérialisés. **Il convient, lors de l'évaluation, d'accorder une importance particulière à la protection des droits fondamentaux par les dispositions du pays tiers et d'autres intérêts fondamentaux, tels les intérêts liés à la sécurité nationale du pays tiers, ainsi que le degré de connexion de l'affaire pénale avec l'une ou l'autre des deux juridictions.**

- (53) Les conditions énoncées à l'article 9 sont également applicables en cas de conflit d'obligations contradictoires découlant de la législation d'un pays tiers. Pendant cette procédure, les données doivent être conservées. Lorsque l'injonction est levée, une nouvelle injonction de conservation peut être émise pour permettre à l'autorité d'émission de demander la production des données par d'autres canaux tels que l'entraide judiciaire.
- (54) Il est essentiel que toutes les personnes dont les données sont demandées dans le cadre d'enquêtes ou de procédures pénales aient accès à un recours juridictionnel effectif, conformément à l'article 47 de la charte des droits fondamentaux de l'Union européenne. Pour les personnes suspectées et accusées, le droit à un recours effectif [...] ***pourrait*** être exercé [...] **lorsque les données obtenues sont utilisées dans le cadre d'une** procédure pénale **engagée contre eux**. Ceci peut affecter la recevabilité ou, le cas échéant, le poids, dans la procédure, de la preuve obtenue de cette manière. Ces personnes bénéficient en outre de toutes les garanties procédurales qui leur sont applicables, tel que le droit à l'information. Les autres personnes **dont les données ont été requises mais** qui ne sont pas suspectées ou accusées devraient également avoir droit à un recours effectif. Par conséquent, la possibilité de contester la légalité d'une injonction européenne de production, notamment la nécessité et la proportionnalité de la décision, doit au minimum être fournie. Le présent règlement ne peut limiter les motifs possibles de contestation de la légalité de l'injonction. Ces recours doivent être exercés dans l'État d'émission conformément à la législation nationale. Les règles relatives aux mesures provisoires doivent être régies par la législation nationale.
- (55) [...] Pendant la procédure de mise en œuvre, **l'autorité chargée de la mise en œuvre peut refuser la reconnaissance et la mise en œuvre d'une injonction européenne de production ou de conservation pour un certain nombre de motifs limités.** [...]
- (56) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. Conformément à l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et à l'article 16, paragraphe 1, du traité FUE, toute personne a droit à la protection des données à caractère personnel la concernant. Lors de la mise en œuvre du présent règlement, les États membres doivent veiller à ce que les données à caractère personnel soient protégées et ne soient traitées qu'en conformité avec le règlement (UE) 2016/679 et la directive (UE) 2016/680.

**(56 bis) La transmission et le transfert ainsi que l'utilisation de preuves électroniques obtenues au moyen d'une injonction européenne de production dans le cadre d'une autre procédure et à d'autres fins que celles pour lesquelles l'injonction a été émise devrait être limitée, en particulier aux infractions pénales pour lesquelles l'autorité d'émission aurait également pu émettre une injonction européenne de production. Par ailleurs, l'utilisation, la transmission ou le transfert de preuves électroniques ne devrait être possible que lorsque les données sont nécessaires pour prévenir une menace grave et immédiate pour la sécurité publique ou les intérêts essentiels de l'État membre ou du pays tiers concerné. Le transfert international de preuves électroniques est en outre soumis aux conditions définies au chapitre V de la directive (UE) 2016/680. Dans les cas où les données à caractère personnel obtenues sont utilisées pour prévenir une menace grave et immédiate pour la sécurité publique ou les intérêts essentiels de l'État membre ou du pays tiers concerné et où ladite menace ne peut déboucher sur une enquête pénale, le règlement (UE) 2016/679 devrait s'appliquer.**

**(56 ter) Lorsqu'ils font une déclaration concernant le régime linguistique, les États membres sont encouragés à indiquer au moins une langue en plus de leur(s) langue(s) officielle(s).**

(57) Les données à caractère personnel obtenues en vertu du présent règlement ne doivent être traitées que lorsque cela est nécessaire et proportionné aux objectifs de prévention, d'enquête, de détection et de poursuite des infractions ou d'exécution des sanctions pénales ainsi que conforme à l'exercice des droits de la défense. Les États membres doivent veiller en particulier à ce que des politiques et mesures appropriées de protection des données s'appliquent à la transmission de données à caractère personnel par les autorités compétentes aux fournisseurs de services aux fins du présent règlement, y compris des mesures garantissant la sécurité des données. Les fournisseurs de services doivent également offrir les mêmes garanties pour la transmission de données à caractère personnel aux autorités compétentes. Seules des personnes autorisées peuvent avoir accès aux informations contenant des données à caractère personnel pouvant être obtenues par des processus d'authentification. L'utilisation de mécanismes garantissant l'authenticité doit être envisagée, comme les systèmes nationaux d'identification électronique notifiés ou les services de confiance tels que prévus par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE.

(58) La Commission doit procéder à une évaluation du présent règlement fondée sur les cinq critères d'efficacité, d'efficacité, de pertinence, de cohérence et de valeur ajoutée de l'UE, qui doit servir de base aux analyses d'impact d'éventuelles mesures supplémentaires. Les informations doivent être collectées régulièrement et notifiées pour l'évaluation du présent règlement.

(59) L'utilisation de formulaires prétraduits et standardisés facilite la coopération et l'échange d'informations entre les autorités judiciaires et les fournisseurs de services, leur permettant de sécuriser et transmettre les preuves électroniques plus rapidement et plus efficacement, tout en répondant aux exigences de sécurité nécessaires d'une manière conviviale. Ces formulaires réduisent les coûts de traduction et contribuent à une norme de qualité élevée. Les formulaires de réponse doivent permettre un échange d'informations normalisées, en particulier lorsque les fournisseurs de services ne peuvent pas se conformer à une demande parce que le compte n'existe pas ou parce qu'aucune donnée n'est disponible. Les formulaires doivent également faciliter la collecte de statistiques.



- (60) Afin de répondre efficacement à un éventuel besoin d'amélioration concernant le contenu des EPOC et des EPOC-PR ainsi que du formulaire à utiliser pour fournir des informations sur l'impossibilité d'exécuter l'EPOC ou l'EPOC-PR, le pouvoir d'adopter les actes en conformité avec l'article 290 du traité sur le fonctionnement de l'Union européenne doit être délégué à la Commission afin de modifier les annexes I, II et III du présent règlement. Il est particulièrement important que la Commission procède aux consultations appropriées pendant ses travaux préparatoires, y compris au niveau des experts, et que ces consultations soient réalisées conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"<sup>18</sup>. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.
- (61) Les mesures basées sur le présent règlement ne remplacent pas les décisions d'enquêtes européennes au titre de la directive 2014/41/UE du Parlement européen et du Conseil<sup>19</sup> visant à obtenir des preuves électroniques. Les autorités des États membres devraient choisir l'outil le plus adapté [...] **en l'espèce**; elles peuvent privilégier l'utilisation de la décision d'enquête européenne pour demander plusieurs types différents de mesures d'enquête, y compris, et sans que cela soit limitatif, la production de preuves électroniques d'un autre État membre.
- (62) Compte tenu des évolutions technologiques, de nouvelles formes d'outils de communication pourraient s'imposer dans quelques années, ou des lacunes pourraient apparaître dans l'application du présent règlement. Il est de ce fait important de prévoir un réexamen de son application.
- (63) Étant donné que l'objectif du présent règlement, à savoir améliorer la collecte et l'obtention de preuves électroniques par-delà les frontières, ne peut pas être réalisé de manière suffisante par les États membres en raison de son caractère transfrontière, mais peut l'être mieux à l'échelle de l'Union, cette dernière peut prendre des mesures conformément au principe de subsidiarité énoncé à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

---

<sup>18</sup> JO L 123 du 12.5.2016, p. 1.

<sup>19</sup> [Directive 2014/41/EU](#) 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).

- (64) Conformément à l'article 3 du protocole sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, [...] l'Irlande a notifié son souhait de participer à l'adoption et à l'application du présent règlement [...] sans préjudice de l'article 4 dudit protocole, le Royaume-Uni [...] ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ou soumis à son application.
- (65) Conformément aux articles 1<sup>er</sup> et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ou soumis à son application.
- (66) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 du Parlement européen et du Conseil<sup>20</sup> et a émis un avis le (...) <sup>21</sup>,

---

<sup>20</sup> Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

<sup>21</sup> JO C du , p. .

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

## Chapitre 1: Objet, définitions et champ d'application

### *Article premier*

#### *Objet*

1. Le présent règlement définit les règles selon lesquelles une autorité d'un État membre peut ordonner à un fournisseur de services qui propose des services dans l'Union de produire ou de conserver des preuves électroniques, quelle que soit la localisation des données. Le présent règlement est sans préjudice des pouvoirs des autorités nationales de contraindre les fournisseurs de services établis ou représentés sur leur territoire à se conformer à des mesures nationales similaires.
2. Le présent règlement n'a pas pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques tels qu'ils sont consacrés à l'article 6 du traité sur l'Union européenne, y compris les droits de la défense des personnes faisant l'objet d'une procédure pénale, et toute obligation qui incombe aux autorités répressives ou policières à cet égard demeure inchangée.

### *Article 2*

#### *Définitions*

Aux fins du présent règlement, on entend par:

- (1) "injonction européenne de production": une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de produire des preuves électroniques;
- (2) "injonction européenne de conservation": une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de conserver des preuves électroniques en vue d'une demande ultérieure de production;
- (3) "fournisseur de services": toute personne physique ou morale qui fournit une ou plusieurs des catégories de services suivants, **à l'exception des services financiers visés à l'article 2, paragraphe 2, point b), de la directive 2006/123/CE**:
  - (a) service de communications électroniques tel que défini à l'article 2, paragraphe 4, de la [directive établissant le code des communications électroniques européen];

- (b) **nom de domaine internet et 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;**
- (c) **autres services de la société de l'information tels que définis à l'article 1<sup>er</sup>, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil<sup>22</sup>, qui:**
  - **offrent à leurs utilisateurs la possibilité de communiquer les uns avec les autres;** ou
  - traitent ou stockent des données pour le compte des utilisateurs auxquels les services sont fournis [...] <sup>23</sup>;
- (4) "proposer des services dans l'Union":
  - (a) permettre à des personnes physiques ou morales dans un ou plusieurs État(s) membre(s) d'utiliser les services énumérés au point 3) ci-dessus; et
  - (b) avoir un lien substantiel **fondé sur des critères factuels spécifiques** avec le ou les États membres visé(s) au point a);
- (5) "établissement" ou "**établi(e(s))**": [...] 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 [...] à partir de laquelle l'entreprise est gérée;
- (6) "preuve électronique": preuve stockée sous forme électronique par un fournisseur de services ou en son nom au moment de la réception d'un certificat d'injonction de production ou de conservation, consistant en données stockées relatives aux abonnés, à l'accès, aux transactions et au contenu;

---

<sup>22</sup> [Directive \(UE\) 2015/1535](#) du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

<sup>23</sup> La Finlande, la Lettonie et le Luxembourg émettent une réserve parce que les autorités publiques ne devraient pas être obligées de se conformer à une injonction européenne de production ou de conservation (Finlande), parce que la définition est toujours trop vague et source d'insécurité juridique (Luxembourg) et parce qu'il convient de réfléchir encore à cette définition, notamment eu égard à la proposition de directive définissant des règles harmonisées pour la désignation de représentants légaux en vue de collecter des preuves dans le cadre de procédures pénales (Lettonie).

- (7) "données relatives aux abonnés": toutes les données relatives à:
- (a) l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, le numéro de téléphone ou le courriel fournis;
  - (b) le type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques liées ou les interfaces utilisées ou fournies par l'abonné ou le client, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou autres moyens d'authentification utilisés à la place d'un mot de passe fournis par un utilisateur ou créés à la demande d'un utilisateur;
- (8) "données relatives à l'accès": les données relatives au début et à la fin d'une session d'accès utilisateur à un service, strictement nécessaires aux seules fins d'identification de l'utilisateur du service, telles que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service, ainsi que l'adresse IP attribuée par le fournisseur de service d'accès à l'internet à l'utilisateur d'un service, les données identifiant l'interface utilisée et l'identifiant de l'utilisateur. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point [...]c), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques];
- (9) "données relatives aux transactions": les données relatives à la fourniture d'un service proposé par un fournisseur de services, qui servent à fournir des informations contextuelles ou supplémentaires sur ce service, et qui sont générées ou traitées par un système d'information du fournisseur de services, tel que la source et la destination d'un message ou d'un autre type d'interaction, les données sur l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, sauf si ces données constituent des données relatives à l'accès. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point [...]c), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques];
- (10) "données relatives au contenu": toutes les données stockées dans un format numérique tel que du texte, de la voix, des vidéos, des images et du son autres que les données relatives aux abonnés, les données relatives à l'accès ou les données relatives aux transactions;
- (11) "système d'information": un système d'information tel que défini à l'article 2, point a), de la directive 2013/40/UE du Parlement européen et du Conseil<sup>24</sup>;
- (12) "État d'émission": l'État membre dans lequel l'injonction européenne de production ou l'injonction européenne de conservation est émise;

---

<sup>24</sup> [Directive 2013/40/UE](#) du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

- (13) "État chargé de la mise en œuvre": l'État membre dans lequel réside ou est établi le destinataire de l'injonction européenne de production ou de l'injonction européenne de conservation et auquel, **au besoin**, l'injonction européenne de production et le certificat d'injonction européenne de production ou l'injonction européenne de conservation et le certificat d'injonction européenne de conservation sont transmis pour mise en œuvre;
- (14) "autorité chargée de la mise en œuvre": l'autorité compétente dans l'État chargé de la mise en œuvre à qui l'injonction européenne de production et le certificat d'injonction européenne de production ou l'injonction européenne de conservation et le certificat d'injonction européenne de conservation sont transmis par l'autorité d'émission pour mise en œuvre;
- (15) "cas d'urgence": les situations où il existe une menace imminente pour la vie ou l'intégrité physique d'une personne ou pour une infrastructure critique telle que définie à l'article 2, point a), de la directive 2008/114/CE du Conseil<sup>25</sup>.

*Article 3*  
*Champ d'application*

1. Le présent règlement s'applique aux fournisseurs de services qui proposent des services dans l'Union.
- 1 bis. Le présent règlement ne s'applique pas aux procédures engagées par l'autorité d'émission en vue de fournir une entraide judiciaire à un autre État membre ou à un pays tiers.**
2. Les injonctions européennes de production et les injonctions européennes [...] **de conservation** ne peuvent être émises que pour des procédures pénales [...] **et pour l'exécution d'une peine ou mesure de sûreté privatives de liberté qui n'a pas été rendue par défaut, au cas où la personne condamnée se soustrait à la justice**[...]. Les injonctions peuvent également être émises dans des procédures relatives à une infraction pénale pour laquelle une personne morale peut être tenue responsable ou sanctionnée dans l'État d'émission.<sup>26</sup>
3. Les injonctions prévues par le présent règlement ne peuvent être émises que pour les données relatives à des services tels que définis à l'article 2, paragraphe 3, proposés dans l'Union.

---

<sup>25</sup> [Directive 2008/114/CE du Conseil](#) du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008 p. 75).

<sup>26</sup> La République tchèque, la Finlande, la Lettonie et l'Allemagne ont émis une réserve sur l'extension du champ d'application en ce qui concerne les personnes condamnées qui se soustraient à la justice. La réserve vaut aussi pour les dispositions parallèles à l'article 5, paragraphe 3, et à l'article 6, paragraphe 2.

## Chapitre 2: Injonction européenne de production, injonction européenne de conservation et certificats

### *Article 4* *Autorité d'émission*

1. Une injonction européenne de production pour les données relatives aux abonnés et les données relatives à l'accès peut être émise par:
  - (a) un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée; ou
  - (b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production en vertu du présent règlement, par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.
2. Une injonction européenne de production pour des données relatives aux transactions et au contenu peut être émise uniquement par:
  - (a) un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée; ou
  - (b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production en vertu du présent règlement, par un juge, une juridiction ou un juge d'instruction dans l'État d'émission.
3. Une injonction européenne de conservation peut être émise par:
  - (a) un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée; ou
  - (b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de conservation est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de conservation en vertu du présent règlement, par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

4. Lorsque l'injonction a été validée par une autorité judiciaire conformément au paragraphe 1, point b), au paragraphe 2, point b), et au paragraphe 3, point b), cette autorité peut également être considérée comme une autorité d'émission aux fins de la transmission du certificat d'injonction européenne de production et du certificat d'injonction européenne de conservation.
5. **Dans les cas d'urgence dont l'existence est établie de manière valable, les autorités mentionnées au paragraphe 1, point b) et au paragraphe 3, point b), peuvent émettre l'injonction pour les données relatives aux abonnés ou l'injonction pour les données relatives à l'accès sans validation préalable si la validation ne peut être obtenue à temps et si ces autorités pourraient émettre l'injonction sans validation dans un cas similaire qui se présenterait sur leur territoire. L'autorité d'émission demande une validation ex post sans retard injustifié, au plus tard dans les 48 heures. Lorsque la validation ex post n'est pas accordée, l'autorité d'émission retire immédiatement l'injonction et, conformément à sa législation nationale, soit supprime toute donnée qui a été obtenue, soit s'assure que les données ne sont pas utilisées en tant que preuve<sup>27</sup>.**
6. **Chaque État membre peut désigner une ou plusieurs autorités centrales chargées de la transmission administrative des certificats, injonctions et notifications, de la réception des données et des notifications ainsi que de la transmission de toute autre correspondance officielle concernant les certificats ou injonctions.**

---

<sup>27</sup> La Grèce et le Luxembourg ont émis une réserve concernant la possibilité de procéder à une validation ex post.



*Article 5*  
*Conditions d'émission d'une injonction européenne de production*

1. Une autorité d'émission ne peut émettre une injonction européenne de production que si les conditions énoncées dans le présent article sont remplies.
2. L'injonction européenne de production est nécessaire et proportionnée aux fins de la procédure visée à l'article 3, paragraphe 2, et ne peut être émise que si une mesure similaire est disponible pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission.
3. Les injonctions européennes de production de données relatives aux abonnés ou de données relatives à l'accès peuvent être émises pour toutes les infractions pénales **ainsi que pour l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois**.
4. Les injonctions européennes de production de données relatives aux transactions ou de données relatives au contenu ne peuvent être émises que<sup>28</sup>:
  - (a) pour des infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins 3 ans<sup>29</sup>, ou
  - (b) pour les infractions suivantes, si elles sont totalement ou partiellement commises au moyen d'un système d'information:
    - les infractions telles que définies aux articles 3, 4 et 5 de la décision-cadre 2001/413/JAI du Conseil<sup>30</sup>;
    - les infractions telles que définies aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil<sup>31</sup>;
    - les infractions telles que définies aux articles 3 à 8 de la directive 2013/40/UE du Parlement européen et du Conseil;

---

<sup>28</sup> La Finlande et la Slovaquie préféreraient qu'il y ait une liste.

<sup>29</sup> Chypre a émis une réserve concernant les conditions d'émission d'une injonction européenne de production pour les infractions pénales punissables d'une peine inférieure à 5 ans.

<sup>30</sup> [Décision-cadre 2001/413/JAI du Conseil](#) du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (JO L 149 du 2.6.2001, p. 1).

<sup>31</sup> [Directive 2011/93/UE](#) du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

(c) pour les infractions pénales telles que définies aux articles 3 à 12 et 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil<sup>32</sup>;

**d) pour l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois prononcée en raison des infractions pénales visées aux points a), b) et c) du présent paragraphe.**

5. L'injonction européenne de production inclut les informations suivantes:

(a) l'autorité d'émission, et, s'il y a lieu, l'autorité de validation;

(b) le destinataire de l'injonction européenne de production visé à l'article 7;

**(c) l'utilisateur, sauf si l'injonction a pour unique but d'identifier l'utilisateur, ou tout autre identifiant unique tel que le nom d'utilisateur, l'identificateur ou le nom du compte afin de déterminer les données qui sont requises [...];**

(d) la catégorie de données requises (données relatives aux abonnés, données relatives à l'accès, données relatives aux transactions ou données relatives au contenu);

(e) s'il y a lieu, la durée pour laquelle la production est requise;

(f) les dispositions applicables du droit pénal de l'État d'émission;

(g) en cas d'urgence ou de demande de divulgation anticipée, les raisons de cette divulgation;

(h) dans les cas où les données requises sont stockées ou traitées dans le cadre d'une infrastructure fournie par un fournisseur de services à une entreprise ou à une entité autre que des personnes physiques, une confirmation que l'injonction a été émise conformément au paragraphe 6;

(i) les motifs de la nécessité et de la proportionnalité de la mesure.

6. Dans le cas où les données requises sont stockées ou traitées dans le cadre d'une infrastructure fournie par un fournisseur de services à une entreprise ou à une entité autre que des personnes physiques, l'injonction européenne de production ne peut être adressée au fournisseur de services que si les mesures d'enquête appliquées à l'entreprise ou à l'entité ne sont pas appropriées, en particulier parce qu'elles pourraient compromettre l'enquête.

---

<sup>32</sup> [Directive \(UE\) 2017/541](#) du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

- 6 bis.** Une injonction européenne de production de données stockées ou traitées dans le cadre d'une infrastructure fournie par un fournisseur de services à une autorité publique ne peut être émise que si l'autorité publique pour laquelle les données sont stockées ou traitées se trouve dans l'État d'émission.
- 7.** [...] Dans les cas où l'injonction concerne des données relatives aux transactions et où l'autorité d'émission [...] est fondée à croire que [...] la personne dont les données sont requises ne réside pas sur le territoire de l'État d'émission, et
- a. les données requises sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État [...] **chargé de la mise en œuvre [...] ou sont soumises, dans cet État membre, à des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, ou** que leur divulgation peut porter atteinte aux intérêts fondamentaux de l'État [...] **chargé de la mise en œuvre**, tels que la sécurité et la défense nationales, l'autorité d'émission [...] demande des éclaircissements sur les circonstances **visées au présent point** avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État [...] **chargé de la mise en œuvre [...]**, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. Si l'autorité d'émission constate que les données requises relatives [...] aux transactions [...] [...] **sont** protégées par ces immunités et privilèges ou **par des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias ou** que leur divulgation porterait atteinte aux intérêts fondamentaux de l'autre État membre, **tels que la sécurité et la défense nationales, elle prend ces circonstances en considération de la même manière que si elles avaient été prévues par sa législation nationale et elle n'émet pas l'injonction européenne de production ou elle l'adapte au besoin pour donner effet à ces motifs.**<sup>33</sup>
- 8.** Lorsque la levée du privilège ou de l'immunité relève d'une autorité de l'État d'émission, l'autorité d'émission peut demander à l'autorité chargée de la mise en œuvre de contacter l'autorité compétente afin de lui demander d'exercer son pouvoir immédiatement. Lorsque la levée du privilège ou de l'immunité relève d'une autorité d'un autre État membre ou d'un pays tiers ou relève d'une organisation internationale, l'autorité d'émission peut demander à l'autorité concernée d'exercer ce pouvoir.

---

<sup>33</sup> L'Allemagne et la République tchèque demandent que les données relatives au contenu soient ajoutées dans cette disposition. L'Allemagne demande quant à elle l'ajout d'une clause relative aux droits fondamentaux, tant dans cette disposition qu'à l'article 12 *bis*. La Hongrie a émis une réserve de fond en raison de la logique qui sous-tend la disposition: selon elle, quand il y a de bonnes raisons de croire qu'un refus est prévisible, une consultation préalable devrait être possible d'une manière générale, également pour les dispositions parallèles à l'article 5, paragraphe 7, à l'article 7 *bis*, à l'article 9, paragraphe 5, et aux articles 12 *bis* et 14.

*Article 6*  
*Conditions d'émission d'une injonction européenne de conservation*

1. Une autorité d'émission ne peut émettre une injonction européenne de conservation que si les conditions énoncées au présent article sont remplies. **L'article 5, paragraphe 6, s'applique mutatis mutandis.**
2. Une injonction européenne de conservation peut être émise si elle est nécessaire et proportionnée pour empêcher le retrait, la suppression ou la modification de données en vue d'une demande ultérieure de production de ces données au moyen de l'entraide judiciaire, d'une décision d'enquête européenne ou d'une injonction européenne de production. Les injonctions européennes de conservation de données peuvent être émises pour toutes les infractions pénales **ainsi que pour l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois.**
3. L'injonction européenne de conservation inclut les informations suivantes:
  - (a) l'autorité d'émission, et, s'il y a lieu, l'autorité de validation;
  - (b) le destinataire de l'injonction européenne de conservation visé à l'article 7;
  - (c) [...] **l'utilisateur**, sauf si l'injonction a pour unique but d'identifier [...] **l'utilisateur, ou tout autre identifiant unique tel que le nom d'utilisateur, l'identificateur ou le nom du compte afin de déterminer les données qui sont requises;**
  - (d) la catégorie de données devant être conservée (données relatives aux abonnés, données relatives à l'accès, données relatives aux transactions ou données relatives au contenu);
  - (e) s'il y a lieu, la durée pour laquelle la conservation est requise;
  - (f) les dispositions applicables du droit pénal de l'État d'émission;
  - (g) les motifs de la nécessité et de la proportionnalité de la mesure.

*Article 7*  
*Destinataire d'une injonction européenne de production et d'une injonction européenne de conservation*

1. L'injonction européenne de production et l'injonction européenne de conservation sont adressées directement à un représentant légal désigné par le fournisseur de services aux fins de la collecte de preuves dans le cadre d'une procédure pénale.
2. Si aucun représentant légal [...] n'a été désigné, l'injonction européenne de production et l'injonction européenne de conservation peuvent être adressées à tout établissement du fournisseur de services dans l'Union.
3. Lorsque le représentant légal ne se conforme pas à un EPOC dans un cas d'urgence en vertu de l'article 9, paragraphe 2, **l'injonction européenne de production** [...] peut être adressée à tout établissement du fournisseur de services dans l'Union.

4. Lorsque le représentant légal ne respecte pas ses obligations en vertu de l'article 9 ou de l'article 10 et que l'autorité d'émission estime qu'il existe un risque sérieux de perte de données, l'injonction européenne de production ou l'injonction européenne de conservation peut être adressée à tout établissement du fournisseur de services dans l'Union.

*Article 7 bis*  
*Notification*<sup>34</sup>

1. **Dans les cas où l'injonction européenne de production concerne des données relatives au contenu et où l'autorité d'émission est fondée à croire que la personne dont les données sont requises ne réside pas sur son propre territoire, l'autorité d'émission soumet une copie de l'EPOC à l'autorité compétente de l'État chargé de la mise en œuvre au moment même où l'EPOC est soumis au destinataire conformément à l'article 7.**
2. **L'autorité notifiée peut, dans les meilleurs délais, informer l'autorité d'émission de toute circonstance visée à l'article 5, paragraphe 7, point b), et elle s'efforce de le faire dans les dix jours. L'autorité d'émission prend ces circonstances en considération de la même manière que si elles avaient été prévues par sa législation nationale et elle retire ou adapte l'injonction au besoin pour donner effet à ces motifs si les données n'ont pas encore été fournies. En cas de retrait, l'autorité d'émission informe immédiatement le destinataire.**
3. **Lorsque la levée du privilège ou de l'immunité relève d'une autorité de l'État d'émission, l'autorité d'émission peut demander à l'autorité notifiée de contacter l'autorité compétente afin de lui demander d'exercer son pouvoir immédiatement. Lorsque la levée du privilège ou de l'immunité relève d'une autorité d'un autre État membre ou d'un pays tiers ou relève d'une organisation internationale, l'autorité d'émission peut demander à l'autorité concernée d'exercer ce pouvoir.**
4. **La notification n'a pas pour effet de suspendre les obligations du destinataire au titre du présent règlement.**

---

<sup>34</sup> La République tchèque, la Finlande, l'Allemagne, la Grèce, la Hongrie et la Lettonie ont émis une réserve sur la procédure de notification, préconisant qu'elle ait davantage d'effets et couvre aussi les données relatives aux transactions et la clause relative aux droits fondamentaux, autrement dit, qu'elle donne à l'autorité notifiée des motifs de refus. Par ailleurs, une logique inverse devrait être retenue pour déterminer ce qu'est un "cas national". Enfin, l'Allemagne préconise que l'injonction soit soumise et non le certificat, tandis que la République tchèque estime qu'il faudrait soumettre les deux. La Belgique, la Bulgarie, l'Estonie, la France, l'Irlande, l'Italie, la Pologne, le Portugal et l'Espagne ont émis une réserve sur la procédure de notification et les dispositions liées à l'introduction d'une telle procédure, en particulier l'article 5, paragraphe 7, et les articles 9, 12 *bis* et 14, ainsi que les considérants correspondants, préférant la formule sans notification de la proposition de la Commission. La Belgique, le Luxembourg, l'Irlande, la Slovaquie et la Pologne préféreraient, à supposer qu'il y ait notification, que celle-ci soit faite à l'État membre dans lequel réside la personne dont les données sont requises.

## Article 8

### *Certificat d'injonction européenne de production et certificat d'injonction européenne de conservation*

1. Une injonction européenne de production ou de conservation est transmise au destinataire tel que défini à l'article 7 au moyen d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR).

L'autorité d'émission ou de validation complète l'EPOC figurant à l'annexe I ou l'EPOC-PR figurant à l'annexe II, le signe et certifie que son contenu est exact et correct.

2. L'EPOC ou l'EPOC-PR est transmis [...] par **ou au nom de l'autorité d'émission [...] d'une manière sécurisée et fiable permettant [...] au destinataire de produire une trace écrite et d'établir [...] l'authenticité du certificat.**

Lorsque les fournisseurs de services, les États membres ou les organes de l'Union ont mis en place des plateformes spéciales ou d'autres canaux sécurisés pour le traitement des demandes de données par les autorités répressives et judiciaires, l'autorité d'émission peut également choisir de transmettre le certificat par ces canaux.

3. L'EPOC contient les informations énumérées à l'article 5, paragraphe 5, points a) à h), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission. Les motifs de la nécessité et de la proportionnalité de la mesure ou d'autres informations concernant les enquêtes ne sont pas inclus.
4. L'EPOC-PR contient les informations énumérées à l'article 6, paragraphe 3, points a) à f), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission. Les motifs de la nécessité et de la proportionnalité de la mesure ou d'autres informations concernant les enquêtes ne sont pas inclus.
5. S'il y a lieu, l'EPOC ou l'EPOC-PR est traduit dans une langue officielle de l'Union acceptée par le destinataire. Si aucune langue n'est spécifiée, l'EPOC ou l'EPOC-PR est traduit dans l'une des langues officielles de l'État membre où le représentant légal réside ou est établi.

*Article 9*  
*Exécution d'un EPOC*

1. Dès réception de l'EPOC, le destinataire veille à ce que les données requises [...] **soient transmises, d'une manière sécurisée et fiable permettant d'établir l'authenticité et l'intégrité**, directement à l'autorité d'émission ou aux autorités répressives comme indiqué dans l'EPOC au plus tard 10 jours après la réception de l'EPOC, sauf si l'autorité d'émission indique les raisons d'une divulgation anticipée<sup>35</sup>.
2. Dans les cas d'urgence, le destinataire transmet les données requises sans retard injustifié au plus tard 6 heures après la réception de l'EPOC.
3. Si le destinataire ne peut pas respecter son obligation parce que l'EPOC est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour son exécution, le destinataire informe l'autorité d'émission mentionnée dans l'EPOC sans retard injustifié et demande des éclaircissements en utilisant le formulaire figurant à l'annexe III. Il indique à l'autorité d'émission si une identification et une conservation sont possibles conformément au paragraphe 6. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Les délais prévus aux paragraphes 1 et 2 ne s'appliquent qu'après la fourniture d'éclaircissements.
4. Si le destinataire ne peut pas respecter son obligation pour cause [...] d'impossibilité de fait **due à des circonstances que le destinataire ou le fournisseur de services n'a pas créées au moment de la réception de l'injonction** [...], le destinataire en informe l'autorité d'émission mentionnée dans l'EPOC sans retard injustifié, en expliquant les raisons au moyen du formulaire figurant à l'annexe III. [...]

---

<sup>35</sup> L'Allemagne propose d'ajouter au minimum un nouveau considérant invitant la Commission et les États membres à mettre au point et à instaurer dans les meilleurs délais des canaux de communication électronique sécurisés permettant d'établir l'authenticité et l'intégrité.

5. Dans tous les cas où le destinataire ne fournit pas les informations requises ou ne les fournit pas de manière exhaustive ou dans les délais, pour d'autres raisons [...], il en informe l'autorité d'émission sans délai injustifié et au plus tard dans les délais prévus aux paragraphes 1 et 2 en utilisant le formulaire figurant à l'annexe III. L'autorité d'émission réexamine l'injonction à la lumière des informations fournies par le fournisseur de services et, si nécessaire, fixe un nouveau délai pour que le fournisseur de services produise les données.

[...] <sup>36</sup>

6. Le destinataire conserve les données requises s'il ne les produit pas immédiatement, à moins que les informations contenues dans l'EPOC ne lui permettent pas d'identifier les données requises, auquel cas il demande des éclaircissements conformément au paragraphe 3. Les données sont conservées jusqu'à leur production, que ce soit sur la base de l'injonction européenne de production clarifiée et de son certificat ou par d'autres canaux, tel que l'entraide judiciaire. Si la production des données et leur conservation ne sont plus nécessaires, l'autorité d'émission et, s'il y a lieu, l'autorité chargée de la mise en œuvre conformément à l'article 14, paragraphe 8, informent le destinataire sans retard injustifié.

---

<sup>36</sup> La Hongrie a émis une réserve sur cette suppression.



*Article 10*  
*Exécution d'un EPOC-PR*

1. Dès réception de l'EPOC-PR, le destinataire conserve les données requises, sans retard injustifié. La conservation prend fin après 60 jours, à moins que l'autorité d'émission ne confirme que la demande ultérieure de production a été introduite.
2. Si l'autorité d'émission confirme dans le délai fixé au paragraphe 1 que la demande ultérieure de production a été introduite, le destinataire conserve les données aussi longtemps que nécessaire pour produire les données une fois la demande de production suivante notifiée.
3. Si la conservation n'est plus nécessaire, l'autorité d'émission en informe le destinataire sans retard injustifié.
4. Si le destinataire ne peut pas respecter son obligation parce que le certificat est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour exécuter l'EPOC-PR, le destinataire en informe l'autorité d'émission figurant dans l'EPOC-PR sans retard injustifié et demande des éclaircissements, en utilisant le formulaire figurant à l'annexe III. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Le destinataire, de son côté, veille à obtenir les éclaircissements nécessaires pour lui permettre de remplir les obligations énoncées au paragraphe 1.
5. Si le destinataire ne peut pas respecter son obligation pour cause [...] d'impossibilité de fait **due à des circonstances que le destinataire ou le fournisseur de services n'a pas créées au moment de la réception de l'injonction** [...], **le destinataire** en [...] **informe** l'autorité d'émission mentionnée dans l'EPOC-PR sans retard injustifié, en expliquant les raisons au moyen du formulaire figurant à l'annexe III. [...]
6. Dans tous les cas où le destinataire ne conserve pas les informations requises, pour d'autres raisons [...], il en informe l'autorité d'émission sans retard injustifié dans le formulaire figurant à l'annexe III. L'autorité d'émission réexamine l'injonction à la lumière de la justification fournie par le fournisseur de services.

*Article 11*  
*Confidentialité et information de l'utilisateur*<sup>37</sup>

1. Les destinataires et, le cas échéant, les fournisseurs de services, prennent les mesures nécessaires pour garantir la confidentialité de l'EPOC ou de l'EPOC-PR ainsi que des données produites ou conservées et [...] s'abstiennent d'informer la personne dont les données sont requises afin **d'éviter** [...] d'entraver la procédure pénale afférente. **Ils n'informent la personne dont les données [...] sont requises que si l'autorité d'émission le demande explicitement. Dans ce cas, l'autorité d'émission fournit également les informations visées au paragraphe 4 du présent article au destinataire ou, s'il ne s'agit pas de la même personne, au fournisseur de services.**
2. Si l'autorité d'émission **n'a pas** demandé au [...] **fournisseur de services** [...] d'informer la personne dont les données **étaient** [...] requises **conformément au paragraphe 1**, elle informe [...] cette personne [...]. [...] **L'autorité d'émission peut différer l'information de la personne dans les données ont été requises pour autant que cette mesure soit nécessaire et proportionnée** [...] pour éviter d'entraver la procédure pénale [...].
3. **L'autorité d'émission peut s'abstenir d'informer la personne dont les données relatives aux abonnés et les données relatives à l'accès ont été requises si cela est nécessaire et proportionné pour protéger les droits fondamentaux et les intérêts légitimes d'une autre personne et, en particulier, lorsque ces droits et intérêts priment sur l'intérêt qu'a la personne dont les données sont requises à être informée.** [...]
4. **Des informations sur les recours disponibles au titre de l'article 17 sont fournies.**

---

<sup>37</sup> La Finlande et l'Allemagne ont émis une réserve, demandant de préciser le texte (dispositions concernant les langues et l'aide juridictionnelle, informations détaillées sur les recours légaux, etc.), l'Allemagne estimant en outre que les personnes concernées (et pas uniquement la personne dont les données sont requises) devraient être informées.

*Article 12*  
*Remboursement des frais*

Le fournisseur de services peut demander à l'État d'émission le remboursement de ses frais, si la législation nationale de l'État d'émission le prévoit pour les injonctions nationales dans des situations similaires, conformément aux dispositions nationales. **Les États membres communiquent les règles de remboursement à la Commission, qui les rend publiques.**

*Article 12 bis [...]*  
*[...] Limitations à l'utilisation des données obtenues*

1. [...] **Au cas où la personne dont les données sont requises ne réside pas sur le territoire de l'État d'émission et où** des données relatives aux transactions ou des données relatives au contenu **ont été** obtenues au moyen de l'injonction européenne de production **et si l'autorité d'émission reçoit des informations indiquant que ces données [...]** sont protégées par des immunités ou des privilèges accordés en vertu de la législation de [...] **l'État [...] chargé de la mise en œuvre [...]** ou **sont soumises, dans l'État chargé de la mise en œuvre, à des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias,** ou [...] si, d'après cet État membre, la divulgation de ces données porterait atteinte à ses intérêts fondamentaux, tels que la sécurité et la défense nationales, [...] **les autorités compétentes** de l'État d'émission garantissent que, pendant la procédure pénale, [...] ces motifs sont pris en considération de la même manière que s'ils avaient été prévus par sa législation nationale [...]. [...] **Les autorités compétentes** peuvent consulter les autorités de l'État membre pertinent, le Réseau judiciaire européen en matière pénale ou Eurojust.
  
2. **Lorsque la levée du privilège ou de l'immunité relève d'une autorité de l'État chargé de la mise en œuvre, l'autorité compétente de l'État d'émission peut demander à l'autorité chargée de la mise en œuvre ou à l'autorité notifiée de contacter l'autorité compétente de l'État chargé de la mise en œuvre afin de lui demander d'exercer son pouvoir immédiatement. Lorsque la levée du privilège ou de l'immunité relève d'une autorité d'un autre État membre ou d'un pays tiers ou relève d'une organisation internationale, l'autorité compétente de l'État d'émission peut demander à l'autorité concernée d'exercer ce pouvoir.**

*Article 12 ter*  
*Principe de spécialité*

1. **Les preuves électroniques ne sont pas utilisées aux fins de procédures autres que celles pour lesquelles elles ont été obtenues conformément au présent règlement, sauf:**
  - a) **aux fins de procédures pour lesquelles une injonction européenne de production aurait pu être émise conformément à l'article 5, paragraphes 3 et 4; ou**
  - b) **pour prévenir une menace grave et immédiate pour la sécurité publique ou les intérêts essentiels de l'État d'émission.**
  
2. **Les preuves électroniques obtenues conformément au présent règlement peuvent uniquement être transmises à un autre État membre:**
  - a) **aux fins de procédures pour lesquelles une injonction européenne de production aurait pu être émise conformément à l'article 5, paragraphes 3 et 4; ou**
  - b) **pour prévenir une menace grave et immédiate pour la sécurité publique ou les intérêts essentiels de cet État membre.**
  
3. **Les preuves électroniques obtenues conformément au présent règlement peuvent uniquement être transférées vers un pays tiers ou à une organisation internationale dans les conditions prévues au paragraphe 2, points a) et b), du présent article et au chapitre V de la directive (UE) 2016/680.**

## Chapitre 3: Sanctions et exécution

### *Article 13* *Sanctions*<sup>38</sup>

Sans préjudice des législations nationales prévoyant l'imposition de sanctions pénales, les États membres fixent les règles relatives aux sanctions pécuniaires applicables aux violations des obligations prévues aux articles 9 et 10 et à l'article 11, **paragraphe 1**, du présent règlement et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Les États membres notifient sans délai ces règles et mesures à la Commission et l'informent sans tarder de toute modification ultérieure les concernant.

Les **États membres veillent à ce que les** sanctions pécuniaires prévues [...] **soient** effectives, proportionnées et dissuasives.

**Les États membres veillent à ce que puissent être imposées des sanctions pécuniaires allant jusqu'à 2 % du chiffres d'affaires annuel mondial total du fournisseur de services pour l'exercice précédent.**

### *Article 14* *Procédure de mise en œuvre*

1. Si le destinataire ne respecte pas un EPOC dans les délais ou un EPOC-PR sans fournir de raisons acceptées par l'autorité d'émission, cette dernière peut transférer à l'autorité compétente de l'État chargé de la mise en œuvre l'injonction européenne de production accompagnée de l'EPOC ou l'injonction européenne de conservation accompagnée de l'EPOC-PR ainsi que le formulaire figurant à l'annexe III rempli par le destinataire et tout autre document pertinent en vue de sa mise en œuvre par tout moyen susceptible de garder une trace écrite dans des conditions permettant à l'autorité chargée de la mise en œuvre d'établir son authenticité. À cette fin, l'autorité d'émission traduit la décision, le formulaire et tout autre document les accompagnant dans l'une des langues [...] [...] **acceptées par cet** État membre et informe le destinataire du transfert.
2. Dès réception, l'autorité chargée de la mise en œuvre reconnaît, sans autres formalités, **et prend les mesures nécessaires à la mise en œuvre**
  - a) d'une injonction européen de production, **à moins que cette autorité ne considère que l'un des motifs prévus au paragraphe 4 s'applique**, ou
  - b) d'une injonction européenne de conservation [...], à moins que cette autorité ne considère que l'un des motifs prévus au paragraphe [...] 5 s'applique [...].

L'autorité chargée de la mise en œuvre décide de reconnaître l'injonction sans retard injustifié et au plus tard dans les 5 jours ouvrables suivant la réception de l'injonction.

---

<sup>38</sup> La Finlande, l'Allemagne et la Lettonie ont émis une réserve concernant l'harmonisation des sanctions.

**2 bis. L'article 5, paragraphe 8, s'applique mutatis mutandis.**

3. Lorsque l'autorité chargée de la mise en œuvre reconnaît l'injonction, elle enjoint formellement au destinataire de se conformer à l'obligation en question, informe ce dernier de la possibilité de s'opposer à la mise en œuvre en invoquant les motifs énumérés au[...] paragraphe[...] 4, **point a) à e)**, ou **au paragraphe 5**, ainsi que des sanctions applicables en cas de non-conformité, et fixe un délai pour qu'il s'y conforme ou qu'il s'y oppose.
4. [...] **La reconnaissance ou** la mise en œuvre de l'injonction européenne de production **ne peut être refusée** que sur la base des motifs suivants:
- (a) l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission prévue à l'article 4;
  - (b) l'injonction européenne de production n'a pas été émise pour une [...] infraction pénale prévue à l'article 5, paragraphe 4;
  - (c) le destinataire n'a pas pu se conformer à l'EPOC en raison d'une impossibilité de fait [...] ou parce que l'EPOC contient des erreurs manifestes;
  - (d) l'injonction européenne de production ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'EPOC;
  - (e) le service n'est pas couvert par le présent règlement;
  - (f) [...] **un des motifs visés à l'article 12 bis, paragraphe 1, s'applique**<sup>39</sup>.
5. [...] **La reconnaissance ou** la mise en œuvre de l'injonction européenne de conservation **ne peut être refusée** que sur la base des motifs suivants:
- (a) l'injonction européenne de conservation n'a pas été émise ou validée par une autorité d'émission prévue à l'article 4;
  - (b) le fournisseur de services n'a pas pu se conformer à l'EPOC-PR en raison d'une impossibilité de fait [...] ou parce que l'EPOC-PR contient des erreurs manifestes;
  - (c) l'injonction européenne de conservation ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'EPOC-PR;
  - (d) le service n'est pas couvert par le champ d'application du présent règlement [...].
  - (e) [...]

---

<sup>39</sup> La République tchèque, la Finlande, la Hongrie, l'Allemagne et la Lettonie ont émis une réserve sur la suppression de l'article 14, paragraphe 4, point f), et paragraphe 5, point e), faisant valoir qu'elles ne pourraient s'y rallier que moyennant l'ajout d'une clause relative aux droits fondamentaux ainsi qu'aux règles constitutionnelles à l'article 5, à l'article 7 bis, paragraphe 2, et à l'article 12 bis, paragraphe 1.

6. En cas d'objection du destinataire **en vertu du paragraphe 4, point a) à e), et du paragraphe 5**, l'autorité chargée de la mise en œuvre décide de mettre en œuvre l'injonction sur la base des informations fournies par le destinataire et, si nécessaire, des informations complémentaires obtenues auprès de l'autorité d'émission conformément au paragraphe 7.
7. Avant de décider de ne pas reconnaître ou de ne pas mettre en œuvre l'injonction conformément aux paragraphes 2 et 6, l'autorité chargée de la mise en œuvre consulte l'autorité d'émission par tout moyen approprié. S'il y a lieu, elle demande des informations complémentaires à l'autorité d'émission. L'autorité d'émission répond à toute demande de ce type dans un délai de 5 jours ouvrables.
8. Toutes les décisions sont notifiées immédiatement à l'autorité d'émission et au destinataire par tout moyen permettant de garder une trace écrite.
9. Si l'autorité chargée de la mise en œuvre obtient les données du destinataire, elle les transmet à l'autorité d'émission dans un délai de deux jours ouvrables, sauf si les données concernées sont protégées par une immunité ou un privilège **ou par des règles sur la détermination et la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias** en vertu de sa propre législation nationale ou si elles portent atteinte à ses intérêts fondamentaux tels que la sécurité et la défense nationales. Dans ce cas, elle informe l'autorité d'émission des raisons pour lesquelles les données n'ont pas été transmises.
10. Si le destinataire ne respecte pas ses obligations en vertu d'une injonction reconnue dont la mise en œuvre a été confirmée par l'autorité chargée de la mise en œuvre, cette autorité inflige une sanction pécuniaire conformément à sa législation nationale. Un recours juridictionnel effectif est disponible contre la décision d'infliger une amende.

## Chapitre 4: Recours

*Article 15*

[...]

[...]



[...]

*Article 16*  
*Procédure de réexamen en cas d'obligations contradictoires [...]*

1. Si le destinataire considère que le respect de l'injonction européenne de production entrerait en conflit avec la législation applicable d'un pays tiers [...], il informe l'autorité d'émission des raisons pour lesquelles il ne peut exécuter l'injonction européenne de production conformément à la procédure visée à l'article 9, paragraphes 5 et 6.
2. L'objection motivée doit inclure toutes les informations pertinentes sur la législation du pays tiers, son applicabilité en l'espèce et la nature de l'obligation contradictoire. Elle ne peut pas être fondée sur le fait que des dispositions similaires concernant les conditions, les formalités et les procédures d'émission d'une injonction de production n'existent pas dans la législation applicable du pays tiers ni sur la seule circonstance que les données sont stockées dans un pays tiers. **Elle est formulée au plus tard dix jours après la date à laquelle l'EPOC a été notifié ou signifié au destinataire. Les délais sont calculés conformément à la législation nationale de l'autorité d'émission.**
3. L'autorité d'émission réexamine l'injonction européenne de production sur la base de l'objection motivée. Si l'autorité d'émission a l'intention de maintenir l'injonction européenne de production, elle demande un réexamen par la juridiction compétente de son État membre. La mise en œuvre de l'injonction est suspendue en attendant la fin de la procédure de réexamen.

4. La juridiction compétente évalue d'abord s'il existe un conflit, en examinant
- (a) si la législation du pays tiers s'applique en fonction des circonstances spécifiques de l'affaire en question et, si tel est le cas,
  - (b) si la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire en question, interdit la divulgation des données concernées.
5. Si la juridiction compétente constate qu'il n'existe pas de conflit pertinent au sens des paragraphes 1 et 4, elle maintient l'injonction. Si la juridiction compétente établit que la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire examinée, interdit la divulgation des données concernées, elle décide s'il y a lieu de maintenir ou de **lever** [...] l'injonction. **Cette évaluation est en particulier fondée** sur [...] les facteurs suivants, **une importance particulière étant accordée aux facteurs visés au points a) et b)**:
- a) l'intérêt protégé par la législation pertinente du pays tiers, y compris les **droits fondamentaux ainsi que d'autres intérêts empêchant la divulgation des données, [...] en particulier les intérêts liés à la sécurité nationale du pays tiers**;
  - b) le degré de connexion de l'affaire pénale pour laquelle l'injonction a été émise avec l'une ou l'autre des deux juridictions, comme l'indiquent entre autres:
    - la localisation, la nationalité et le lieu de résidence de la personne dont les données sont requises et/ou de la(des) victime(s),
    - le lieu où l'infraction pénale en question a été commise;
  - c) le degré de connexion entre le fournisseur de services et le pays tiers en question. Dans ce contexte, le lieu de stockage des données en tant que tel ne suffit pas à établir un degré substantiel de connexion;
  - d) l'intérêt de l'État enquêteur à obtenir les preuves concernées, en fonction de la gravité de l'infraction et de l'importance d'obtenir rapidement des preuves;
  - e) les éventuelles conséquences pour le destinataire ou le fournisseur de services s'il se conforme à l'injonction européenne de production, y compris les sanctions qu'il peut encourir.

- 5 ter.** La juridiction peut solliciter des informations auprès de l'autorité compétente du pays tiers, compte tenu de la directive (UE) 2016/680, en particulier son chapitre V, et dans la mesure où la transmission de ces informations n'entrave pas la procédure pénale afférente.
6. Si la juridiction compétente décide de lever l'injonction, elle en informe l'autorité d'émission et le destinataire. Si la juridiction compétente décide que l'injonction doit être maintenue, elle informe l'autorité d'émission et le destinataire, lequel procède à la mise en œuvre de l'injonction.

*Article 17*  
*Recours effectifs<sup>40</sup>*

1. **Sans préjudice d'autres recours légaux disponibles conformément à la législation nationale, toute** [...] personne [...] dont les données ont été **requisées** [...] au moyen d'une injonction européenne de production a droit à des recours effectifs contre l'injonction européenne de production. **Lorsqu'il s'agit d'une personne suspectée [...] ou accusée, elle a droit à des recours effectifs** pendant la procédure pénale [...] dans le cadre de laquelle [...] **les données ont été utilisées. Ces recours sont** sans préjudice des recours disponibles en vertu de la directive (UE) 2016/680 et du règlement (UE) 2016/679.
2. [...]
3. Ce droit à un recours effectif est exercé devant une juridiction de l'État d'émission conformément à la législation de cet État et comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité.

---

<sup>40</sup> L'Allemagne a émis une réserve, faisant valoir que toute personne concernée par une injonction devrait avoir droit à un recours et pas uniquement la personne dont les données ont été requises et que les recours devraient également être possibles dans le cadre de procédures pénales contre des injonctions de conservation.

4. Sans préjudice de l'article 11, l'autorité d'émission prend les mesures appropriées pour veiller à ce que des informations sur les possibilités de recours prévues par la législation nationale soient fournies et pour garantir qu'elles sont exercées de manière effective.
5. Les mêmes délais ou autres conditions pour la formation d'un recours dans des affaires nationales similaires s'appliquent ici et d'une manière qui garantit l'exercice effectif de ces recours pour les personnes concernées.
6. Sans préjudice des règles de procédure nationales, les États membres garantissent que pour les procédures pénales dans l'État d'émission, les droits de la défense et l'équité de la procédure sont respectés lors de l'évaluation des preuves obtenues au moyen de l'injonction européenne de production.

*Article 18*  
[...]

[...]

## Chapitre 5: Dispositions finales

### *Article 18 bis* *Régime linguistique*

**Chaque État membre indique s'il accepte une ou plusieurs langues outre sa ou ses langues officielles et, dans l'affirmative, lesquelles, pour la transmission d'un EPOC ou d'un EPOC-PR et/ou d'une injonction européenne de production et d'une injonction européenne de conservation en cas de mise en œuvre.**

### *Article 19* *Suivi et rapports*

1. Le [*date d'application du présent règlement*] au plus tard, la Commission établit un programme détaillé pour le suivi des résultats, des conséquences et des incidences du présent règlement. Le programme de suivi définit par quels moyens et dans quels intervalles les données et autres éléments de preuve nécessaires seront collectés. Il précise quelles mesures la Commission et les États membres doivent prendre pour collecter et analyser les données et autres preuves.
2. En tout état de cause, les États membres collectent et conservent les statistiques détaillées obtenues des autorités compétentes. Les données collectées sont transmises à la Commission chaque année avant le 31 mars pour l'année civile précédente et comprennent, **dans la mesure du possible**:
  - (a) le nombre d'EPOC et d'EPOC-PR émis par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non, **validation ex post**);
  - (b) le nombre d'EPOC exécutés ou non exécutés par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non);
  - (c) pour les EPOC exécutés, la durée moyenne pour l'obtention des données requises depuis le moment où l'EPOC est émis jusqu'au moment où les données sont obtenues, par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non);

- (d) le nombre d'injonctions européenne de production transmises à un État chargé de la mise en œuvre et reçues pour mise en œuvre par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non) ainsi que le nombre d'injonctions mises en œuvre;
- (e) le nombre de recours légaux formés contre les injonctions européennes de production dans l'État d'émission et dans l'État chargé de la mise en œuvre par type de données requises;
- (f) **le nombre de cas où la validation ex post n'a pas été accordée.**

**3. Les fournisseurs de services peuvent collecter, conserver et publier des statistiques; si tel est le cas, les données peuvent être transmises à la Commission avant le 31 mars pour l'année civile précédente et peuvent comprendre, dans la mesure du possible:**

- (a) **le nombre d'EPOC et d'EPOC-PR reçus par type de données requises, les États membres et la situation (cas d'urgence ou non);**
- (b) **le nombre d'EPOC exécutés ou non exécutés par type de données requises, les États membres et la situation (cas d'urgence ou non);**
- (c) **pour les EPOC exécutés, la durée moyenne pour la fourniture des données requises depuis le moment où l'EPOC est reçu jusqu'au moment où les données sont fournies, par type de données requises, les États membres et la situation (cas d'urgence ou non).**

#### *Article 20*

#### *Modifications des certificats et des formulaires*

La Commission adopte des actes délégués conformément à l'article 21 pour modifier les annexes I, II et III afin de répondre efficacement à une éventuelle nécessité d'améliorer le contenu des formulaires EPOC et EPOC-PR et des formulaires à utiliser pour fournir des informations sur l'impossibilité d'exécuter l'EPOC ou l'EPOC-PR.

*Article 21*  
*Exercice de la délégation*

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
2. La délégation de pouvoir visée à l'article 20 est conférée pour une durée indéterminée à compter du [*date d'application du présent règlement*].
3. La délégation de pouvoir visée à l'article 20 peut être révoquée à tout moment par le Parlement européen ou par le Conseil. Une décision de révocation met fin à la délégation de pouvoir spécifiée dans la décision. La révocation prend effet le jour suivant celui de la publication de la décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.
4. Avant d'adopter un acte délégué, la Commission consulte des experts désignés par chaque État membre conformément aux principes énoncés dans l'accord interinstitutionnel "Mieux légiférer" du 13 avril 2016<sup>41</sup>.
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.
6. Un acte délégué adopté en vertu de l'article 20 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de 2 mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prorogé de 2 mois à l'initiative du Parlement européen ou du Conseil.

---

<sup>41</sup> JO L 123 du 12.5.2016, p. 13.

*Article 22*  
*Notifications*

1. Le [*date d'application du présent règlement*] au plus tard, chaque État membre notifie à la Commission ce qui suit:
  - (a) les autorités qui, conformément à sa législation nationale, sont compétentes, conformément à l'article 4, pour émettre, [...] valider, **transmettre et/ou recevoir** des injonctions européennes de production et des injonctions européennes de conservation **ou les notifications y afférentes**;
  - (b) l'autorité chargée de la mise en œuvre ou les autorités qui sont compétentes pour mettre en œuvre les injonctions européennes de production et les injonctions européennes de conservation pour le compte d'un autre État membre;
  - (c) les juridictions compétentes pour traiter les objections motivées des destinataires conformément [...] **à l'article 16**;
  - (d) **les langues acceptées pour la transmission de l'EPOC ou de l'EPOC-PR et/ou d'une injonction européenne de production et d'une injonction européenne de conservation en cas de mise en œuvre conformément à l'article 18 bis**.
2. La Commission publie les informations reçues au titre du présent article, soit sur un site internet spécifique, soit sur le site internet du Réseau judiciaire européen visé à l'article 9 de la décision 2008/976/JAI du Conseil<sup>42</sup>.

*Article 23*  
*Rapport avec [...] d'autres instruments, accords et arrangements*

**Le présent règlement ne porte pas atteinte aux autres instruments, accords et arrangement de l'UE et au niveau international relatifs à [...] la collecte de preuves qui relèveraient également du champ d'application du présent règlement.**

---

<sup>42</sup> Décision 2008/976/JAI du Conseil du 16 décembre 2008 relative au Réseau judiciaire européen (JO L 348 du 24.12.2008, p. 130).



*Article 24*  
*Évaluation*

Le [5 ans à compter de la date d'application du présent règlement] au plus tard, la Commission procède à une évaluation du règlement et présente un rapport au Parlement européen et au Conseil sur le fonctionnement du présent règlement, qui comprend une évaluation de la nécessité d'élargir son champ d'application. Si cela s'avère nécessaire, le rapport est accompagné de propositions législatives. L'évaluation est réalisée conformément aux lignes directrices de la Commission pour une meilleure réglementation. Les États membres fournissent à la Commission les informations nécessaires à l'élaboration de ce rapport.

*Article 25*  
*Entrée en vigueur*

Le présent règlement entre en vigueur le vingtième jour suivant sa publication au *Journal officiel de l'Union européenne*.

Il s'applique à compter du [...] **24 mois après son entrée en vigueur**].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Strasbourg, le

*Par le Parlement européen*

*Le président*

*Par le Conseil*

*Le président*

---