



Document de séance

A9-0256/2020

11.12.2020

*****I**

RAPPORT

sur la proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale
(COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteuse: Birgit Sippel

Légende des signes utilisés

- * Procédure de consultation
- *** Procédure d'approbation
- ***I Procédure législative ordinaire (première lecture)
- ***II Procédure législative ordinaire (deuxième lecture)
- ***III Procédure législative ordinaire (troisième lecture)

(La procédure indiquée est fondée sur la base juridique proposée par le projet d'acte.)

Amendements à un projet d'acte

Amendements du Parlement présentés en deux colonnes

Les suppressions sont signalées par des *italiques gras* dans la colonne de gauche. Les remplacements sont signalés par des *italiques gras* dans les deux colonnes. Le texte nouveau est signalé par des *italiques gras* dans la colonne de droite.

Les première et deuxième lignes de l'en-tête de chaque amendement identifient le passage concerné dans le projet d'acte à l'examen. Si un amendement porte sur un acte existant, que le projet d'acte entend modifier, l'en-tête comporte en outre une troisième et une quatrième lignes qui identifient respectivement l'acte existant et la disposition de celui-ci qui est concernée.

Amendements du Parlement prenant la forme d'un texte consolidé

Les parties de textes nouvelles sont indiquées en *italiques gras*. Les parties de texte supprimées sont indiquées par le symbole ■ ou barrées. Les remplacements sont signalés en indiquant en *italiques gras* le texte nouveau et en effaçant ou en barrant le texte remplacé.

Par exception, les modifications de nature strictement technique apportées par les services en vue de l'élaboration du texte final ne sont pas marquées.

SOMMAIRE

	Page
PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN	5
PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND	67
VOTE FINAL PAR APPEL NOMINAL EN COMMISSION COMPÉTENTE AU FOND ..	68

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale
(COM(2018)0225 – C8-0155/2018 – 2018/0108(COD))

(Procédure législative ordinaire: première lecture)

Le Parlement européen,

- vu la proposition de la Commission au Parlement européen et au Conseil (COM(2018)0225),
 - vu l'article 294, paragraphe 2, et l'article 82, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, conformément auxquels la proposition lui a été présentée par la Commission (C8-0155/2018),
 - vu l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne,
 - vu l'article 59 de son règlement intérieur,
 - vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A9-0256/2020),
1. arrête la position en première lecture figurant ci-après;
 2. demande à la Commission de le saisir à nouveau si elle remplace, modifie de manière substantielle ou entend modifier de manière substantielle sa proposition;
 3. charge son Président de transmettre la position du Parlement au Conseil et à la Commission ainsi qu'aux parlements nationaux.

Amendement 1

AMENDEMENTS DU PARLEMENT EUROPÉEN*

à la proposition de la Commission

Proposition de

* Amendements: le texte nouveau ou modifié est signalé par des italiques gras; les suppressions sont signalées par le symbole ■.

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif aux injonctions européennes de production et de conservation *d'informations électroniques dans les procédures pénales*

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 européen¹,

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 *informations* 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 *informations* électroniques sont *essentiels* pour lutter contre la criminalité, sous réserve de conditions *et de garanties* garantissant *la pleine conformité aux* droits *et aux* principes fondamentaux reconnus dans *l'article 6 du traité sur l'Union européenne (traité UE) et* la charte des droits fondamentaux de l'Union européenne (*ci-après la «charte»*), et en particulier les principes de nécessité et de proportionnalité, de légalité, de protection de la vie privée *et des données à caractère personnel, et de confidentialité des communications*.
- (3) █
- (4) █
- (5) █
- (6) █

¹ JO C., p..

- (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 ***où les services sont fournis. Par conséquent, les informations électroniques pertinentes*** sont souvent ***stockées*** hors de l'État menant l'enquête, ***ce qui rend plus difficile la collecte d'informations électroniques dans les procédures pénales.***
- (8) C'est pourquoi des demandes de coopération judiciaire sont souvent adressées à des États qui hébergent un grand nombre de fournisseurs de services. En outre, le nombre de demandes a considérablement augmenté. En conséquence, l'obtention ***d'informations*** électroniques par les canaux de coopération judiciaire prend souvent beaucoup de temps, ***ce qui peut poser des problèmes en raison de la nature souvent éphémère des informations électroniques.*** Il n'existe par ailleurs pas de cadre ***harmonisé*** 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 ***de plus en plus*** sur ***les canaux*** de coopération ***volontaire directe*** avec les fournisseurs de services lorsqu'il existe, en ***appliquant*** différents outils nationaux et différentes conditions et procédures nationales.
- (9) La fragmentation du cadre juridique crée des défis pour ***les services répressifs, les autorités judiciaires et*** les fournisseurs de services qui cherchent à se conformer aux demandes ***émanant de la justice, car ils se heurtent de plus en plus souvent à l'incertitude juridique et, potentiellement, à des conflits de lois.*** Par conséquent, il est nécessaire de proposer ***des règles spécifiques sur la conservation et la production d'informations électroniques dans le cadre de la coopération judiciaire transfrontière pour compléter le droit de l'Union actuel et préciser les modalités de la coopération entre les services répressifs, les autorités judiciaires et les fournisseurs de services en matière d'informations électroniques, dans le plein respect de l'État de droit et des droits fondamentaux et principes énoncés à l'article 6 du traité UE et dans la charte.***
- (9 bis) ***La directive 2014/41/UE du Parlement européen et du Conseil² prévoit l'acquisition de preuves, l'accès à ces preuves et leur production dans un État membre en vue d'enquêtes et de procédures pénales dans un autre État membre. Les procédures et délais prévus dans la décision d'enquête européenne pourraient ne pas convenir pour les informations électroniques, qui sont plus éphémères et pourraient être plus rapidement et facilement supprimées. Le présent règlement prévoit donc des procédures spécifiques applicables à la nature des informations électroniques. Toutefois, afin d'éviter une fragmentation à long terme du cadre de l'Union pour la coopération judiciaire en matière pénale, la Commission devrait, à moyen terme, évaluer le fonctionnement du règlement par rapport à la directive 2014/41/UE.***
- (10) █
- (10 bis) ***Le présent règlement respecte les droits fondamentaux et observe les***

² ***Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).***

principes inscrits à l'article 6 du traité sur l'Union européenne, dans la charte, dans le droit international et les accords internationaux auxquels l'Union ou l'ensemble des États membres sont parties, y compris la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et dans les constitutions des États membres dans leur champ d'application respectif. Ces droits et principes comprennent notamment le respect de la vie privée et familiale, la protection des données à caractère personnel, 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.

- (10 ter) Aucune disposition du présent règlement ne doit être interprétée comme interdisant de refuser l'exécution d'une injonction européenne de production lorsqu'il y a des raisons de croire, sur la base d'éléments objectifs, que cette injonction a été émise dans le but de poursuivre ou de punir une personne en raison de son sexe, de ses origines ethniques, de sa religion, de son orientation sexuelle, de son identité de genre, de sa nationalité, de sa langue ou de ses opinions politiques, ou qu'elle pourrait lui être préjudiciable sur la base de l'un de ces motifs.*
- (11) Le mécanisme des injonctions européennes de production et de conservation d'informations électroniques dans les *procédures* pénales fonctionne sur un principe de confiance mutuelle entre les États membres *et une présomption de respect par les autres États membres du droit de l'Union et, notamment, des droits fondamentaux, qui sont des éléments essentiels de l'espace de liberté, de sécurité et de justice au sein de l'Union. Toutefois, si l'autorité d'exécution a des motifs sérieux de croire que la mise en œuvre d'une injonction européenne de production serait incompatible avec ses obligations concernant la protection des droits fondamentaux reconnus dans l'article 6 du traité UE et dans la charte, l'exécution de l'injonction européenne de production devrait être refusée. Avant de décider de soulever l'un des motifs de non-reconnaissance ou de non-exécution prévus par le présent règlement, l'autorité d'exécution devrait consulter l'autorité d'émission pour obtenir toute information complémentaire nécessaire. Les informations relatives à des défaillances systémiques ou généralisées constatées à la suite d'une proposition motivée de la Commission au Conseil, telle que visée à l'article 7, paragraphes 1 et 2, du traité UE, devraient faire l'objet d'une attention particulière aux fins de cette évaluation.*
- (11 bis) Si le Conseil européen devait adopter une décision constatant, comme le prévoit l'article 7, paragraphe 2, du traité UE, l'existence d'une violation grave et persistante, dans l'État membre d'émission, des principes énoncés à l'article 2 du traité UE, tels que ceux inhérents à l'état de droit, l'autorité judiciaire d'exécution peut décider automatiquement de soulever l'un des motifs de non-reconnaissance ou de non-exécution prévus par le présent règlement, sans devoir procéder à une évaluation spécifique.*
- (11 ter) Le respect de la vie privée et familiale ainsi que la protection des personnes physiques à l'égard du traitement des données à caractère personnel constituent des droits fondamentaux. Conformément à l'article 7 et à l'article 8, paragraphe 1, de la charte et à l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications ainsi qu'à la protection des données à caractère*

personnel la concernant. Lors de la mise en œuvre du présent règlement, les États membres devraient veiller à ce que les données à caractère personnel soient uniquement protégées et traitées conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil³, à la directive (UE) 2016/680 du Parlement européen et du Conseil⁴, et à la directive 2002/58/CE du Parlement européen et du Conseil⁵.

(11 quater) Les données à caractère personnel obtenues en vertu du présent règlement ne devraient être traitées que lorsque cela est nécessaire, d'une manière proportionnée aux objectifs de prévention, d'enquête, de détection et de poursuite des infractions, ou d'exécution des sanctions pénales, et conformément à l'exercice des droits de la défense. Les États membres devraient veiller en particulier à ce que des politiques et des mesures appropriées de protection des données, y compris des mesures garantissant la sécurité 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. Les fournisseurs de services devraient également offrir les mêmes garanties pour la transmission de données à caractère personnel aux autorités compétentes. Seules des personnes autorisées devraient avoir accès aux informations contenant des données à caractère personnel.

(12) █

(13) █

(13 bis) Selon la jurisprudence de la Cour de justice de l'Union européenne, la conservation générale et indifférenciée des données par les autorités nationales de sécurité de l'Union porte gravement atteinte aux règles en matière de respect de la vie privée inscrites notamment dans la charte. L'application du présent règlement ne devrait par conséquent pas avoir pour effet d'entraîner une conservation générale et indifférenciée des données, ni d'affecter les droits ou obligations des fournisseurs de services en ce qui concerne la sécurité des données, dont le droit au chiffrement.

(14) █ Les droits procéduraux énoncés dans les directives 2010/64/UE⁶, 2012/13/UE⁷,

³ *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).*

⁴ *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).*

⁵ *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive relative à la vie privée et aux communications électroniques) (JO L 201 du 31.7.2002, p. 37).*

⁶ *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).*

⁷ *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).*

2013/48/UE⁸, (UE) 2016/343⁹, (UE) 2016/800¹⁰ et (UE) 2016/1919¹¹ du Parlement européen et du Conseil *devraient s'appliquer, dans les limites du champ d'application de ces directives, aux procédures pénales relevant du présent règlement en ce qui concerne les États membres liés par les directives en question. Les garanties procédurales prévues par la charte s'appliquent à toutes les procédures relevant du présent règlement.*

- (14 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 doit consulter les autorités de cet État membre conformément à la décision-cadre 2009/948/JAI du Conseil¹².*
- (15) Le présent instrument fixe les règles selon lesquelles, *dans une procédure pénale*, 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 *informations* électroniques *pouvant servir d'éléments de preuve* au moyen d'une injonction européenne de production ou de conservation. Le présent règlement s'applique dans tous les cas *transfrontières* où le fournisseur de services est établi *principalement dans un autre État membre* ou, *s'il n'est pas établi dans l'Union, est légalement* représenté dans un autre État membre. *Les autorités des États membres ne devraient pas émettre d'injonctions nationales ayant des incidences extraterritoriales pour la production ou la conservation d'informations électroniques pouvant faire l'objet d'une demande au titre du présent règlement.*
- (16) Les fournisseurs de services les plus pertinents pour *la collecte d'informations électroniques dans le cadre de* 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 directive (UE) 2018/1972 du Parlement européen et du Conseil¹³ ■**. Ces services incluent les moyens de communication interpersonnelle tels que la voix par le protocole de l'internet (IP), la

⁸ 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).

⁹ 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).

¹⁰ 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).

¹¹ 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).

¹² *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 *Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).*

messagerie instantanée et les services de courrier électronique. Les catégories de services de la société de l'information incluses **dans le présent règlement** sont celles pour lesquelles le stockage de données est une composante déterminante du service fourni à l'utilisateur, et concernent en particulier les réseaux sociaux dans la mesure où ils ne sont pas considérés comme des services de communication électronique, les places de marché en ligne facilitant les transactions entre leurs utilisateurs (tels que des consommateurs ou des entreprises) et les autres services d'hébergement, notamment lorsque le service est fourni par l'intermédiaire de l'informatique en nuage.

(17) █

(18) Les fournisseurs de services d'infrastructure internet liés à l'attribution de noms et de numéros, tels que les registraires et registres de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire ou les registres internet régionaux répertoriant les adresses IP, revêtent un intérêt particulier lorsqu'il s'agit d'identifier les acteurs à l'origine de sites web malveillants ou corrompus. Ils détiennent des données qui **pourraient permettre** d'identifier une personne ou une entité cachée derrière un site internet utilisé dans une activité criminelle, ou la victime d'une activité criminelle.

(18 bis) Les injonctions au titre du présent règlement destinées à des fournisseurs de services qui ne sont pas établis dans l'un des États membres liés par le présent règlement devraient être adressées à leur principal établissement ou à leurs représentants légaux désignés à cet effet. L'établissement principal d'un fournisseur de services établi dans plusieurs États membres est le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens de fourniture des services soient prises dans un autre établissement du fournisseur de services dans l'Union et que ce dernier établissement ait le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions doit être considéré comme l'établissement principal.

(19) Le présent règlement régit **uniquement** la collecte des données stockées au moment **de l'émission** d'une 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 l'émission** d'une **injonction européenne** de production ou de conservation.

(20) Les catégories de données couvertes par le présent règlement comprennent les données relatives aux abonnés, les données relatives **au trafic** et les données relatives au contenu. **Ces catégorisations sont conformes au droit de nombreux États membres, au droit de l'Union, notamment la directive 2002/58/CE, à la jurisprudence de la Cour de justice de l'Union européenne, et au droit international, notamment la convention sur la cybercriminalité du Conseil de l'Europe (STCE n° 185) (ci-après «convention de Budapest»).**

(21) Il y a donc lieu de distinguer les données relatives **aux abonnés** comme une catégorie de données spécifique utilisée dans le présent règlement. Les données relatives **aux abonnés** sont demandées pour identifier l'utilisateur sous-jacent, et le niveau d'interférence avec les droits fondamentaux **est inférieur à celui d'autres catégories de données plus sensibles.**

(22) D'autre part, les données relatives **au trafic** sont généralement demandées pour obtenir des informations **portant davantage atteinte à la vie privée, telles que** les contacts de

l'utilisateur et le lieu où il se trouve, et peuvent servir à établir le profil *complet* d'une personne concernée. *Par conséquent, eu égard à leur sensibilité, les données relatives au trafic sont comparables aux données relatives au contenu.*

(22 bis) Les adresses IP peuvent constituer un élément de départ essentiel pour les enquêtes pénales dans lesquelles l'identité d'un suspect n'est pas connue. Conformément à l'acquis de l'Union tel qu'interprété par la Cour de justice de l'Union européenne, les adresses IP doivent être considérées comme des données à caractère personnel et bénéficiant de la protection complète prévue en matière de protection des données dans le cadre de cet acquis. Dans certains cas, elles peuvent aussi être considérées comme des données relatives au trafic. Toutefois, aux fins d'une enquête pénale spécifique, les services répressifs peuvent demander l'adresse IP d'un utilisateur dans le seul but de l'identifier et, à une étape ultérieure, le nom ou l'adresse de l'abonné ou de l'utilisateur enregistré. Dans ce cas, il convient d'appliquer le même régime que pour les données relatives aux abonnés, tel que défini dans le présent règlement.

(22 ter) Les métadonnées peuvent être traitées et analysées plus facilement que les données relatives au contenu, puisqu'elles apparaissent déjà dans un format structuré et normalisé, mais peuvent également révéler des informations très sensibles et à caractère personnel lorsqu'elles sont dérivées de services ou de protocoles de communications électroniques. Il est donc essentiel de considérer les métadonnées d'autres services ou protocoles de communications électroniques comme des données relatives au contenu lorsqu'elles sont stockées, transmises, distribuées ou échangées lors de l'utilisation de ces services ou par les fournisseurs de ces services.

(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. *L'incidence sur les droits fondamentaux est toutefois plus ou moins importante selon les catégories*, en particulier entre les informations relatives aux abonnés d'une part, et les données relatives *au trafic* et celles relatives au contenu d'autre part. Si les données relatives aux abonnés et *les adresses IP* peuvent être utiles pour obtenir les premiers indices dans une enquête sur l'identité d'un suspect, les données relatives *au trafic* et au contenu sont *souvent plus* pertinentes en tant qu'éléments de preuve *susceptibles de conduire à sa condamnation*. 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 *garanties et des conditions* différentes sont imposées pour obtenir *de telles données*.

(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 *concernant* une infraction pénale concrète qui a déjà été commise, après une évaluation individuelle de la proportionnalité et de la nécessité dans chaque cas, *en tenant compte des droits du suspect ou de la personne poursuivie*.

(25) **I**

(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.

- (27) Pour déterminer si un fournisseur de services fournit des services dans l'Union, il est nécessaire d'évaluer *s'il a clairement l'intention de fournir ses services aux personnes concernées, physiques ou morales*, dans un ou plusieurs États membres *de l'Union*. Toutefois, la seule accessibilité d'une interface en ligne, comme par exemple l'accessibilité d'un site internet, d'une adresse électronique *ou* d'autres coordonnées *d'un fournisseur de services ou d'un intermédiaire, ou bien l'utilisation d'une langue également utilisée dans un État membre, doit être considérée comme insuffisante pour confirmer cette intention*.
- (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 doit être évalué sur la base de l'existence d'un nombre significatif d'utilisateurs dans un ou plusieurs États membres, ou du ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités sur un ou plusieurs États membres *devrait* être établi sur la base de l'ensemble des circonstances pertinentes, notamment des facteurs tels que le recours à une langue ou à une devise utilisée généralement dans cet État membre ou la possibilité de commander des biens ou des services ■.
- (28 bis) Les situations où une menace imminente pèse sur la vie ou l'intégrité physique d'une personne devraient être traitées comme des cas d'urgence et permettre de raccourcir les délais pour le fournisseur de services et l'autorité d'exécution. Les situations où l'arrêt ou la destruction d'une infrastructure critique ferait peser directement un risque imminent sur la vie ou l'intégrité physique d'une personne devraient également être considérées comme des cas d'urgence, conformément au droit de l'Union.*
- (29) Une injonction européenne de production ne doit être émise que si elle s'avère nécessaire et proportionnée *en tenant compte des droits des personnes suspectées ou accusées ainsi que de la gravité de l'infraction*. L'évaluation devrait déterminer si *cette injonction aurait pu être ordonnée dans les mêmes conditions dans une affaire nationale similaire, s'il existe des raisons suffisantes de croire qu'une infraction a été commise, si cette infraction est suffisamment grave pour justifier la production transfrontière des données et si les informations demandées sont pertinentes pour l'enquête*. L'injonction *devrait être* limitée à ce qui est *strictement* nécessaire pour atteindre l'objectif légitime d'obtenir les données pertinentes et nécessaires pour servir de preuve uniquement dans le cas d'espèce *et devrait être limitée aux données de personnes précises ayant un lien direct avec la procédure spécifique en cours*. *L'existence d'un lien direct entre la personne dont les données sont demandées et l'objet de la procédure spécifique doit pouvoir être démontrée à tout moment*.
- (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 *au trafic* 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 étant moins sensibles, des injonctions européennes de production pour leur divulgation peuvent également être émises ou validées par des procureurs compétents *et capables d'exercer cette responsabilité de*

manière objective. Lorsque le droit national le prévoit, l'exécution de l'injonction peut nécessiter l'intervention d'une juridiction de l'État d'exécution.

- (30 bis) *L'autorité d'émission compétente ne devrait être considérée comme indépendante que si elle ne risque pas, au moment d'adopter une décision, d'être soumise, directement ou indirectement, à des directives ou instructions externes, émanant notamment de l'exécutif, par exemple d'un ministre de la justice. Cette indépendance devrait être réputée exister lorsque, sur la base de la législation appropriée et d'un cadre institutionnel, l'autorité d'émission compétente est en mesure d'exercer ses responsabilités de manière objective et agit en toute indépendance dans l'exercice de ses responsabilités inhérentes à l'émission d'une injonction européenne de production ou de conservation, en tenant compte de tous les éléments à charge et à décharge et sans risquer d'être soumise à des directives ou instructions externes dans le cadre de son pouvoir de décision.*
- (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 d'adresses IP aux seules fins d'identification d'une personne* peuvent être émises pour toute infraction pénale, tandis que l'accès aux données relatives *au trafic* et 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 un certain nombre d'autres conditions et garanties ex ante et ex post prévues dans *le présent règlement* 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 *informations* 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 *du Parlement européen et du Conseil*¹⁴, *et les infractions relatives aux abus sexuels et à l'exploitation sexuelle des enfants, telles*

¹⁴ *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).*

que décrites dans la directive 2011/93/UE du Parlement européen et du Conseil¹⁵, ne requièrent pas de seuil relatif à une durée maximale d'emprisonnement d'au moins trois ans.

(33) █

(34) █

(35) Les immunités et privilèges, qui peuvent concerner des catégories de personnes (comme les diplomates) ou des relations spécifiquement protégées (comme le secret professionnel *ou la confidentialité des sources*), *de même que les règles relatives à la liberté de la presse et à la liberté d'expression dans d'autres médias*, sont mentionnés dans d'autres instruments de reconnaissance mutuelle comme la décision d'enquête européenne. *Il n'y a pas de définition commune de ce qui constitue une immunité ou un privilège dans le droit de l'Union. C'est donc au droit des différents États membres de définir précisément ces termes. Il peut s'agir de protections qui s'appliquent aux professions médicales (comme les médecins) et juridiques, au clergé ou à d'autres conseillers protégés, mais aussi de règles relatives à la liberté de la presse et à la liberté d'expression dans d'autres médias (tels que celles couvrant les journalistes), même si cela n'est pas toujours considéré comme une forme de privilège ou d'immunité. Par conséquent, le droit national applicable devrait déjà être pris en compte au moment de l'émission de l'injonction, étant donné que l'autorité d'émission ne peut émettre l'injonction que si elle aurait pu l'être sous les mêmes conditions dans une affaire nationale similaire.* Outre ce principe de base, les immunités et privilèges protégeant les données dans l'État *d'exécution* doivent être pris en considération dans la mesure du possible dans l'État d'émission de la même manière que s'ils étaient prévus dans la législation nationale de l'État d'émission. Ceci est particulièrement pertinent si la législation de l'État *d'exécution* prévoit une protection plus élevée que la législation de l'État d'émission. Afin d'offrir une garantie supplémentaire, ces aspects doivent être pris en considération non seulement lors de l'émission de l'injonction, mais également plus tard, *au cours de la procédure de notification ou* lors de l'évaluation de la pertinence et de la recevabilité des données concernées au stade pertinent de la procédure pénale, et si une procédure d'exécution est engagée par l'autorité d'*exécution*.

(36) Une injonction européenne de conservation de données peut être émise pour toutes les infractions *pénales, si elle aurait pu être demandée sous les mêmes conditions dans une affaire nationale similaire dans l'État d'émission, lorsqu'il existe des raisons suffisantes pour penser qu'une infraction pénale a été commise, qu'elle est suffisamment grave pour justifier la conservation transfrontière des données et que les informations demandées sont pertinentes pour l'enquête. Elle est limitée aux données de personnes spécifiques ayant un lien direct avec les procédures spécifiques visées dans le présent règlement, et le lien direct entre la personne dont les données sont demandées et la finalité du traitement spécifique doit pouvoir être démontré à tout moment. L'objectif des injonctions européennes de conservation est d'empêcher l'effacement, la suppression ou la modification des données concernées lorsque leur production risque de prendre plus de temps.*

¹⁵ 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).

- (37) Les injonctions européennes de production et de conservation doivent être adressées à *l'établissement principal du fournisseur de services où se situe le responsable du traitement, ou, dans le cas d'un fournisseur de services non établi sur le territoire de l'Union ou d'un État membre lié par le présent règlement, à son représentant légal désigné par le fournisseur de services. Parallèlement, elles doivent être adressées directement à l'autorité d'exécution.*
- (38) Les injonctions européennes de production et de conservation doivent être transmises au moyen d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR). Les certificats doivent contenir les mêmes informations obligatoires que les injonctions. Le cas échéant, le certificat *devrait* être traduit dans la ou les langues officielles, ou dans l'une des langues officielles de l'État *d'exécution et du fournisseur de services*, ou dans une autre langue officielle explicitement acceptée par *l'État membre ou le fournisseur de services. À cet égard, les États membres doivent être autorisés, à tout moment, à indiquer dans une déclaration déposée auprès de la Commission qu'ils acceptent des traductions des EPOC et des EPOC-PR dans une ou plusieurs langues officielles de l'Union autres que la ou les langues officielles de l'État membre concerné. La Commission devrait mettre ces déclarations à la disposition de tous les États membres et du Réseau judiciaire européen en matière pénale.*
- (39) L'autorité d'émission compétente devrait transmettre l'EPOC ou l'EPOC-PR directement *aux destinataires, par l'intermédiaire d'un système européen commun d'échange numérique mis en place par la Commission au plus tard le [date d'application du présent règlement]. Ce système devrait permettre la mise en place de canaux sécurisés pour le traitement des communications transfrontalières autorisées, de l'authentification et de la transmission des injonctions et des données demandées entre les autorités compétentes et les fournisseurs de services, en garantissant un échange efficace, fiable et fluide des informations pertinentes, un niveau élevé de sécurité, de confidentialité et d'intégrité ainsi que la protection nécessaire de la vie privée et des données à caractère personnel conformément au règlement (UE) 2018/1725 du Parlement européen et du Conseil¹⁶, au règlement (UE) 2016/679, à la directive (UE) 2016/680 et à la directive 2002/58/CE. À cette fin, des technologies de pointe, ouvertes et couramment utilisées en matière de signature électronique et de chiffrement devraient être employées. Ce système devrait également permettre aux destinataires de produire un document écrit dans des conditions qui leur permettent d'établir l'authenticité de l'injonction et de l'autorité d'émission, conformément aux règles protégeant les données à caractère personnel.*
- (39 bis) Lorsque les fournisseurs de services ou les États membres ont déjà mis en place des systèmes spécifiques ou d'autres canaux sécurisés pour le traitement des demandes de données à des fins répressives, il devrait être possible de connecter ces systèmes ou canaux au système européen commun d'échange numérique.*
- (40) *Dès réception d'un EPOC pour les données relatives aux abonnés ou les adresses IP dans le seul but d'identifier une personne, le fournisseur de services devrait veiller à ce que les données demandées soient transmises à l'autorité d'émission au plus tard*

¹⁶ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, JO L 295 du 21.11.2018, p. 39.

dans les 10 jours suivant la réception de l'EPOC *et dans les 16 heures en cas d'urgence. Lorsque l'autorité d'exécution décide d'invoquer l'un des motifs de non-reconnaissance ou de non-exécution énumérés dans le présent règlement dans les délais impartis, elle devrait immédiatement informer l'autorité d'émission et le fournisseur de services de sa décision. L'autorité d'émission devrait effacer les données. Lorsque les données demandées n'ont pas encore été transmises à l'autorité d'émission, le fournisseur de services destinataire ne peut pas transmettre les données.*

(40 bis) Lorsqu'il reçoit un EPOC pour les données relatives au trafic ou aux contenus, le fournisseur de services devrait tout mettre en œuvre pour conserver les données demandées. Lorsque l'autorité d'exécution invoque l'un des motifs de non-reconnaissance ou de non-exécution énumérés dans le présent règlement dans les délais impartis, elle devrait immédiatement informer l'autorité d'émission et le fournisseur de services de sa décision. Lorsque l'État d'émission fait l'objet d'une procédure visée à l'article 7, paragraphe 1 ou paragraphe 2, du traité UE, le fournisseur de services ne devrait transmettre les données demandées qu'après en avoir reçu l'autorisation écrite explicite de la part de l'autorité d'exécution. Sans préjudice de cette disposition spécifique, si l'autorité d'exécution n'a invoqué aucun des motifs énumérés dans le présent règlement dans les délais impartis, le fournisseur de services devrait s'assurer que les données demandées sont immédiatement et directement transmises à l'autorité d'émission ou aux autorités répressives comme indiqué dans l'EPOC.

(41) █

(42) Lorsqu'il reçoit un certificat d'injonction européenne de conservation (EPOC-PR), le fournisseur de services doit *tout mettre en œuvre pour* conserver les données demandées pendant 60 jours au maximum. *La période de 60 jours est calculée pour permettre l'introduction d'une demande officielle de production. Elle ne peut être prolongée que de 30 jours, et uniquement lorsque cela est nécessaire pour permettre une évaluation supplémentaire de la pertinence des données dans l'enquête en cours, afin d'éviter la perte de données potentiellement pertinentes avant l'expiration de l'injonction européenne de conservation. Si l'autorité d'émission transmet ensuite aux destinataires l'injonction européenne de production dans les délais impartis, le fournisseur de services doit continuer de conserver les données aussi longtemps que nécessaire pour pouvoir exécuter l'injonction européenne de production.*

(42 bis) Afin de permettre au fournisseur de services de résoudre d'éventuels problèmes, dans les cas où l'EPOC ou l'EPOC-PR serait incomplet, sur le fond ou sur la forme, ou contiendrait des erreurs manifestes ou des informations insuffisantes pour l'exécution de l'injonction, il est nécessaire de prévoir une procédure de communication, permettant de demander des éclaircissements ou, le cas échéant, une correction de la part de l'autorité d'émission. En outre, il peut arriver que le fournisseur de services soit incapable de donner les informations requises, pour cause de force majeure ou d'impossibilité de fait qui ne lui est pas imputable, ou ne puisse pas les donner de manière exhaustive ou en temps utile pour toute autre raison. Ces raisons peuvent être techniques ou opérationnelles, comme dans le cas des restrictions opérationnelles des petites et moyennes entreprises. Dans de pareilles situations, le fournisseur de services devrait également en aviser les

autorités d'émission et fournir les justifications appropriées; il en va de même s'il juge l'injonction manifestement abusive ou excessive. Par exemple, une injonction demandant la production de données appartenant à une catégorie indéterminée de personnes dans une zone géographique ou n'ayant aucun lien avec une procédure pénale précise ignorerait manifestement les conditions d'émission d'une injonction européenne de production ou de conservation. La procédure de communication doit donc largement permettre la correction ou le réexamen de l'EPOC ou de l'EPOC-PR par l'autorité d'émission à un stade précoce. Si des éclaircissements ou une correction sont nécessaires, l'autorité d'émission doit réagir rapidement et dans un délai de 5 jours au plus tard. En l'absence de réaction de la part de l'autorité d'émission, l'injonction devrait être considérée comme nulle et non avenue. Si les conditions pertinentes sont remplies, l'autorité d'émission devrait fixer un nouveau délai ou retirer l'injonction. Pour garantir la disponibilité des données, le fournisseur de services devrait conserver les données demandées pendant le temps de la procédure, lorsque cela est possible.

(42 ter) Nonobstant le principe de confiance mutuelle, l'autorité d'exécution devrait avoir la possibilité de refuser la reconnaissance de l'exécution d'une injonction européenne de production, lorsque ce refus est fondé soit sur l'absence des conditions d'émission d'une telle injonction, telles que définies par le présent règlement, soit sur d'autres motifs particuliers énumérés dans le présent règlement.

(42 quater) Le principe non bis in idem est un principe de droit fondamental dans l'Union, reconnu par la charte et développé par la jurisprudence de la Cour de justice. Par conséquent, lorsque l'autorité d'exécution évalue une injonction européenne de production, elle devrait refuser son exécution lorsque celle-ci est contraire à ce principe.

(42 quinquies) De surcroît, lorsque l'autorité d'exécution évalue une injonction européenne de production et qu'il existe des motifs sérieux de croire que l'exécution de cette injonction serait incompatible avec les obligations de l'État membre au titre de l'article 6 du traité UE et de la charte, l'autorité d'exécution devrait refuser l'exécution de cette injonction.

(42 sexies) En outre, lorsque la reconnaissance ou l'exécution d'une injonction européenne de production impliquerait la violation d'une immunité ou d'un privilège dans l'État d'exécution, l'autorité d'exécution devrait refuser cette injonction lorsqu'elle l'évalue.

(42 septies) En raison du caractère plus intrusif des injonctions européennes de production pour les données relatives au trafic et au contenu, l'autorité d'exécution devrait disposer de motifs facultatifs supplémentaires de non-reconnaissance et de non-exécution pour ces catégories de données.

(43) L'information de la personne dont les données sont demandées étant un élément essentiel en matière de droits relatifs à la protection des données et de droits de la défense, car elle permet un contrôle effectif et un recours juridictionnel, conformément à l'article 6 du traité UE et à la charte, le fournisseur de service devrait informer la personne dont les données sont demandées dans les meilleurs délais. Pour ce faire, le fournisseur de services devrait adopter les mesures opérationnelles et techniques de pointe qui se révèlent nécessaires pour garantir la sécurité, la confidentialité et l'intégrité de l'EPOC ou de l'EPOC-PR ainsi que des

données produites ou conservées.

(43 bis) Aussi longtemps qu'elle le juge nécessaire et proportionné pour éviter d'entraver la procédure pénale concernée ou pour protéger les droits fondamentaux d'une autre personne, et en tenant dûment compte de l'incidence de la mesure sur les droits fondamentaux de la personne dont les données sont demandées, l'autorité d'émission peut demander au fournisseur de services de s'abstenir d'informer la personne dont les données sont demandées, sur la base d'une injonction judiciaire, qui doit être dûment justifiée, préciser la durée de l'obligation de confidentialité et faire l'objet d'un réexamen périodique. Si l'autorité d'émission a demandé au fournisseur de services de s'abstenir d'informer la personne, l'autorité d'émission informe sans retard injustifié la personne dont les données sont demandées au sujet de la production ou de la préservation des données. Cette information peut être retardée aussi longtemps qu'elle le juge nécessaire et proportionné, compte tenu des droits du suspect et de la personne poursuivie, sans préjudice des droits de la défense et de l'existence effective de voies de recours. L'information de l'utilisateur doit comprendre des informations relatives à l'ensemble des voies de recours visées dans le présent règlement.

(43 ter) Les informations électroniques obtenues conformément au présent règlement ne doivent pas être utilisées aux fins de procédures autres que celles pour lesquelles elles ont été obtenues conformément au présent règlement, sauf en cas de menace imminente pour la vie ou l'intégrité physique d'une personne. Les situations où l'arrêt ou la destruction d'une infrastructure critique ferait peser directement un risque imminent sur la vie ou l'intégrité physique d'une personne devraient également être considérées comme des menaces imminentes pour la vie ou l'intégrité physique d'une personne, conformément au droit de l'Union.

(43 quater) Les informations électroniques recueillies en violation de l'une des conditions énumérées dans le présent règlement doivent être effacées sans délai. Les informations électroniques qui ne sont plus nécessaires à l'enquête ou aux poursuites pour lesquelles elles ont été produites ou conservées, y compris aux éventuels recours, doivent également être immédiatement effacées, à moins que cela n'affecte les droits de la défense de la personne suspectée ou poursuivie. À cette fin, il faut prévoir des réexamens périodiques de la nécessité de stocker les informations électroniques. La personne dont les données ont été demandées doit être informée de l'effacement.

(43 quinquies) Les informations électroniques recueillies en violation du présent règlement doivent être irrecevables devant une juridiction. Cela doit également s'appliquer aux situations dans lesquelles les critères établis dans le présent règlement ne sont pas réunis. Lorsque des informations électroniques ont été obtenues avant qu'un motif de non-reconnaissance énuméré dans le présent règlement n'ait été invoqué, elles doivent également être irrecevables devant une juridiction. Lors de l'évaluation de l'admissibilité d'informations électroniques obtenues conformément au présent règlement, les autorités judiciaires compétentes doivent, à toutes les étapes de la procédure, veiller au respect des droits de la défense et du caractère équitable de la procédure. Aux fins de cette évaluation, les autorités judiciaires compétentes doivent également examiner soigneusement si les critères énumérés dans le présent règlement sont réunis, en particulier lorsqu'il est possible que les données demandées soient protégées par des immunités ou des privilèges.

(43 sexies) Lorsque le fournisseur de services le réclame, l'État d'émission doit rembourser les coûts justifiés supportés par le fournisseur et liés à l'exécution de l'injonction européenne de production ou l'injonction européenne de conservation. À cette fin, les États membres doivent communiquer les règles de remboursement à la Commission, qui doit les rendre publiques. Lorsque des raisons pratiques, telles que la taille économique du fournisseur de services ou la différence de régime linguistique ou de réglementation nationale relative au remboursement des frais entre l'État d'émission et l'État d'exécution, empêchent substantiellement le fournisseur de services de demander à l'État d'émission le remboursement des frais liés à l'exécution d'une injonction européenne de production ou d'une décision d'enquête européenne, le fournisseur de services doit être en droit de demander le remboursement des frais à l'État d'exécution. Lorsque le fournisseur de services choisit l'État d'exécution, l'État d'émission doit rembourser ces frais à l'État d'exécution.

(43 septies) Les États membres devraient fixer les règles relatives aux sanctions encourues en cas de violation des obligations prévues par le présent règlement. Ces sanctions devraient être effectives, proportionnées et dissuasives. Lorsqu'elles déterminent les sanctions appropriées encourues en cas de violation de la part des fournisseurs de services, 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 ait été commise intentionnellement ou par négligence et le fait que le fournisseur de services ait déjà été tenu responsable d'infractions similaires. À cet égard, une attention particulière devrait être accordée aux microentreprises.

(43 octies) Lorsqu'un fournisseur de services agit avec une diligence raisonnable, notamment en ce qui concerne les obligations en matière de protection des données, et demande des éclaircissements ou des justifications à l'autorité d'émission conformément au présent règlement, il ne devrait pas être tenu responsable des conséquences d'un quelconque retard que cela aurait occasionné. En outre, les sanctions prononcées en cas de violation des obligations incombant au fournisseur de services dans le cadre du présent règlement devraient être annulées lorsqu'il a été fait droit à la contestation d'une injonction conformément au présent règlement.

(44) Lorsque le fournisseur de services ne respecte pas un EPOC ou un EPOC-PR dans les délais impartis sans fournir de raisons suffisantes et lorsque, dans le cas d'un EPOC, l'autorité d'exécution n'a invoqué aucun des motifs énumérés dans le présent règlement, l'autorité d'émission peut demander à l'autorité compétente de l'État d'exécution d'exécuter l'injonction. Dans ce cas, l'État d'exécution devrait formellement demander au fournisseur de services de respecter l'injonction et lui indiquer qu'il a la possibilité de contester cette exécution en invoquant l'un des motifs à la disposition du fournisseur de services pour demander la correction ou le réexamen de l'injonction, conformément au présent règlement. Lorsqu'un fournisseur de services continue à ne pas respecter ses obligations, les États membres devraient prononcer des sanctions conformément au présent règlement.

(45) █

(46) █

(47) En plus des personnes dont les données sont *demandées*, le droit d'un pays tiers peut être affecté par la mesure d'enquête. *Dans de telles situations, la coopération judiciaire*

fondée sur des accords internationaux constitue généralement le moyen le plus approprié de demander des informations électroniques en cas de conflit juridique avec un pays tiers. Sans préjudice des accords internationaux en la matière et 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 si le fournisseur de services ou l'autorité d'exécution considère que la conformité avec une injonction européenne de production ou une injonction européenne de conservation serait en contradiction avec le droit applicable d'un pays tiers interdisant la divulgation des données en question.

- (48) À cette fin, chaque fois que le fournisseur de service ou l'autorité d'exécution considère que dans un cas spécifique, l'injonction européenne de production ou de conservation entraînerait la violation d'une obligation découlant de la législation d'un pays tiers, il doit en informer l'autorité d'émission *et les destinataires concernés sans délai, et au plus tard dans les dix jours à compter de la réception de l'injonction, ce qui suspend l'exécution de celle-ci. Cette notification doit comprendre tous les détails pertinents sur la législation du pays tiers, son applicabilité en l'espèce et la nature de l'obligation contradictoire.* L'autorité d'émission doit alors examiner l'injonction européenne de production ou de conservation, dans les dix jours suivant la réception de l'avis, en tenant compte de critères tels que les intérêts protégés par le droit applicable, le lien entre l'affaire pénale et le pays tiers, le lien entre le fournisseur de services et le pays tiers, les intérêts de l'État d'émission d'obtenir les informations électroniques et les conséquences éventuelles pour les destinataires s'ils se conforment à l'injonction européenne de production ou de conservation. Au cours de cette procédure, les données demandées devraient être conservées lorsque cela est possible.
- (48 bis) *L'autorité d'émission doit avoir la possibilité de retirer, de maintenir ou d'adapter l'injonction si nécessaire, afin d'appliquer les critères pertinents. En cas de retrait, l'autorité d'émission en informe immédiatement les destinataires. Lorsque l'autorité d'émission décide de maintenir l'injonction, elle en informe les destinataires. L'autorité d'exécution, tout en tenant dûment compte de la décision de l'autorité d'émission, doit prendre une décision finale fondée sur les critères énumérés dans le présent règlement, dans les dix jours suivant la réception de la décision de l'autorité d'émission, et doit en informer l'autorité d'émission et le fournisseur de services.*
- (49) Pour déterminer l'existence d'une obligation contradictoire dans les circonstances spécifiques de l'affaire examinée, *l'autorité d'émission et l'autorité d'exécution doivent solliciter des informations auprès de l'autorité compétente du pays tiers*, par exemple si le réexamen soulève des questions sur l'interprétation de la législation du pays tiers concerné, *conformément à la directive (UE) 2016/680, dans la mesure où cela n'entrave pas les délais prévus par le présent règlement.*

(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 **de la législation d'un** 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, **afin de pouvoir** 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) █

(52) █

(53) █

(54) █ Conformément à l'article 47 de la charte, ***il est essentiel que toutes les personnes dont les données ont été demandées en vertu d'une injonction européenne de production ou de conservation aient le droit à un recours effectif contre ces injonctions dans l'État d'émission ou dans l'État d'exécution conformément au droit national, y compris la possibilité de contester la légalité, la nécessité et la proportionnalité d'une injonction, et ce, sans préjudice des recours disponibles en vertu du règlement (UE) 2016/679 et de la directive (UE) 2016/680. Les raisons de fond qui ont conduit à l'émission d'une injonction européenne de production ou de conservation doivent être contestées dans l'État d'émission, sans préjudice des garanties des droits fondamentaux dans l'État d'exécution. L'autorité d'émission et l'autorité d'exécution doivent prendre les mesures appropriées afin de veiller à ce que des informations sur les possibilités de recours légaux prévus par le droit national soient communiquées en temps utile, notamment pour déterminer à quel moment ces recours deviennent applicables et pour garantir la possibilité de leur exercice effectif.***

(55) █

(56) █

(57) █

(57 bis) Afin de suivre les résultats, conséquences et incidences du présent règlement, la Commission devrait publier un rapport annuel portant sur l'année civile précédente, à partir des données collectées auprès des États membres. À cette fin, les États membres devraient rassembler et maintenir des statistiques complètes obtenues auprès des autorités compétentes sur différents volets du présent règlement, classées par type de données demandées, par destinataire (autorité exécutive concernée), par type de fournisseur de services [services de communications électroniques, services de la société de l'information, noms de domaine internet et services de numérotation IP (tels que les fournisseurs d'adresses IP, les registres et registres de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire associés)] ainsi qu'en fonction du caractère urgent ou non de l'affaire. Le cas échéant, les données rassemblées devraient également inclure les motifs invoqués pour la non-

reconnaissance ou non-exécution, les recours déposés, les sanctions imposées, les frais déclarés par le fournisseur de services et la procédure d'exécution engagée.

- (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'Union, qui doit servir de base aux analyses d'impact *et examiner l'utilisation des dérogations (dérogations d'urgence et dérogations au principe de l'information de l'utilisateur), le bon fonctionnement du système européen commun d'échange et l'application satisfaisante du présent règlement en lien avec la directive 2014/41/UE* ■. 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 *différentes* autorités judiciaires *ainsi qu'avec* les fournisseurs de service, et permet *de transmettre des informations électroniques plus rapidement et plus efficacement* d'une manière conviviale. Ces formulaires *peuvent aussi réduire* les coûts de traduction et *contribuer* à une norme de qualité élevée. Les formulaires de réponse doivent permettre un échange d'informations normalisées. Les formulaires doivent également faciliter la collecte de statistiques.
- (60) ■
- (61) Les mesures fondées sur le présent règlement ne devraient pas remplacer les décisions d'enquêtes européennes au titre de la directive 2014/41/UE ■ *ni les procédures d'entraide judiciaire* visant à obtenir des *informations* électroniques. Les autorités des États membres doivent choisir l'outil le plus adapté à leur situation; 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 *d'informations* électroniques d'un autre État membre.
- (62) ■
- (63) Étant donné que l'objectif du présent règlement, à savoir améliorer la collecte et l'obtention *d'informations* 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 *cet objectif*.
- (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 et, 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^{er} 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 **42, paragraphe 2**, du règlement **(UE) 2018/1725** du Parlement européen et du Conseil¹⁷ et a rendu un avis le **6 novembre 2019**¹⁸.

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

¹⁷ *Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE, JO L 295 du 21.11.2018, p. 39.*

¹⁸ *Avis 7/2019 du Contrôleur européen de la protection des données sur des propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (6 novembre 2019).*

Chapitre 1: Objet, définitions et champ d'application

Article premier

Objet

1. Le présent règlement définit les règles selon lesquelles, ***dans le cadre d'une procédure pénale***, une autorité d'un État membre peut ordonner à un fournisseur de services proposant des services dans l'Union ***et établi ou, s'il n'est pas établi, légalement représenté dans un autre État membre***, de produire ou de conserver des ***informations*** électroniques ***pouvant servir de preuves***, quelle que soit la localisation des données.
Les autorités des États membres n'émettent pas d'injonctions nationales ayant des incidences extraterritoriales pour la production ou la conservation d'informations électroniques pouvant faire l'objet d'une demande au titre du présent règlement.
- 1 bis. Dans le cadre des droits de la défense applicables conformément à la procédure pénale nationale, l'émission d'une injonction européenne de production ou de conservation peut également être demandée au nom d'un suspect ou d'une personne poursuivie.***
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 ***dans la charte et 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 judiciaires ainsi qu'aux fournisseurs de service*** à cet égard demeure inchangée.

Article 2:

Définitions

Aux fins du présent règlement, on entend par:

- (1) «injonction européenne de production»: une décision ***qui a été émise ou validée*** par une autorité ***judiciaire*** d'un État membre (***l'«État d'émission»***) ***adressée à*** un fournisseur de services proposant des services dans l'Union et établi ou ***légalement représenté dans un autre État membre soumis au présent règlement (l'«État d'exécution»)***, ***dans l'objectif de produire des informations*** électroniques;
- (2) «injonction européenne de conservation»: une décision judiciaire ***qui a été émise ou validée*** par une autorité ***judiciaire*** d'un État membre (***«l'État d'émission»***) ***adressée à*** un fournisseur de services proposant des services dans l'Union et établi ou ***légalement représenté dans un autre État membre soumis au présent règlement («l'État d'exécution»)***, ***dans l'objectif de conserver des informations*** 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 suivantes ***et qui agit en tant que responsable du***

traitement des données au sens du règlement (UE) 2016/679, pour ce qui est des données à caractère personnel:

- a) des services de communications électroniques tels que définis à l'article 2, paragraphe 4, de la [directive établissant le code des communications électroniques européen];
 - b) services de la société de l'information tels que définis à l'article premier, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil¹⁹ pour lesquels le stockage de données est un élément déterminant du service fourni à l'utilisateur ■;
 - c) 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'enregistrement fiduciaire associés;
- (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)***; et
 - b) avoir un lien substantiel avec le ou les États membres visé(s) au point a); ***il y a lieu de considérer qu'un lien substantiel avec l'Union existe lorsque le fournisseur de services dispose d'un établissement dans l'Union ou, dans le cas contraire, sur la base de l'existence d'un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou du ciblage des activités sur un ou plusieurs États membres;***
- (5) «établissement ***principal***»: ***en ce qui concerne un fournisseur de services établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens de traitement des données ne soient prises dans un autre établissement du fournisseur de services dans l'Union et que ce dernier établissement ait le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;***
- (6) «***informations électroniques***»: ***données relatives aux abonnés, au trafic ou au contenu stockées légalement par un fournisseur de services au moment de l'émission d'une injonction européenne de production ou de conservation, qui sont demandées pour servir d'éléments de preuve lors d'une enquête, de poursuites et de procédures judiciaires concernant une infraction pénale dans un État membre, conformément au droit national;***
- (7) «données relatives aux abonnés»: toutes les données ***collectées dans le cadre de l'activité normale de l'entreprise relatives au nom, à la date de naissance, à l'adresse postale ou géographique, aux données de facturation et de paiement, au numéro de***

¹⁹ [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.

téléphone ou au courriel fournis, qui permettent d'identifier l'abonné ou le client, ainsi que le type de services fournis et la durée du contrat avec le fournisseur de services, et qui sont strictement nécessaires aux seules fins d'identification de l'utilisateur du service;

(8) «données relatives **au trafic**»: les données *collectées dans le cadre de l'activité normale de l'entreprise* relatives **■**:

a) *au type de service fourni et à sa durée, en ce qui concerne les données techniques et les données identifiant les mesures techniques liées ou les interfaces utilisées par l'abonné ou le client ou qui lui sont fournies, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou d'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;*

b) *au début et à la fin d'une session d'accès utilisateur à un service, telle que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service;*

c) *aux métadonnées de communications électroniques traitées dans un réseau de communications électroniques à des fins de transmission, de distribution ou d'échange de contenu de communications électroniques, y compris des données permettant de remonter jusqu'à la source et la destination d'une communication et de les identifier, des données relatives à l'emplacement de l'équipement terminal traitées dans le cadre de la fourniture de services de communications électroniques, ainsi que la date, l'heure, la durée et le type de communication;*

(9) **■**

(10) «données relatives au contenu»: toutes les données stockées *par le fournisseur de services* 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 ou les données relatives au *trafic*;

(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 Conseil²⁰;

(12) «État d'émission»: l'État membre dans lequel l'injonction européenne de production ou de conservation est émise;

(12 bis) «autorité d'émission»: l'autorité de l'État d'émission compétente dans l'affaire concernée pour émettre l'injonction européenne de production ou de conservation;

(13) «État d'exécution»: l'État membre dans lequel est établi *ou légalement représenté le fournisseur de services* et auquel l'injonction européenne de production et le certificat d'injonction européenne de production ou l'injonction européenne de conservation et

²⁰ [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.

le certificat d'injonction européenne de conservation sont transmis pour **notification et mise en œuvre de l'injonction conformément au présent règlement**;

- (14) «autorité **d'exécution**»: l'autorité compétente dans l'État **d'exécution** 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 notification et mise en œuvre de l'injonction conformément au présent règlement, lorsque le droit national le prévoit, l'autorité d'exécution peut être une autorité judiciaire de l'État d'exécution**;
- (15) «cas d'urgence»: les situations où il existe une menace imminente pour la vie ou l'intégrité physique d'une personne.

Article 3

Champ d'application

1. Le présent règlement s'applique **aux États membres et** aux fournisseurs de service qui proposent des services **dans un ou plusieurs États membres soumis au présent règlement, et qui sont établis ou représentés légalement dans l'un de ces États membres**.
- 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 **dans le cadre et aux fins de** procédures pénales, tant durant la phase d'instruction que pendant le procès. 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.
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.

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

Article 4

Autorité d'émission

1. Une injonction européenne de production **visant à obtenir des** données relatives aux abonnés et **des adresses IP aux seules fins de la détermination de l'identité de personnes précises ayant un lien direct avec les procédures explicitement visées à l'article 3, paragraphe 2**, peut être émise par:

- a) un juge, une juridiction, un juge d'instruction ou un procureur compétent 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 *au trafic* et au contenu peut être émise uniquement par:
- a) un juge, une juridiction ou un juge d'instruction compétent 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 *pour toutes les catégories de données* peut être émise par:
- a) un juge, une juridiction, un juge d'instruction ou un procureur compétent 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 transmission du certificat d'injonction européenne de production et du certificat d'injonction européenne de conservation.

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, **compte tenu des droits de la personne concernée. Elle ne peut être émise que si elle peut être demandée sous les mêmes conditions dans une affaire nationale similaire et lorsqu'il existe des raisons suffisantes pour penser qu'une infraction pénale a été commise, qu'elle est suffisamment grave pour justifier la production transfrontière des données et que les informations demandées sont pertinentes pour l'enquête. Elle se limite aux données des personnes précises ayant un lien direct avec les procédures explicitement visées à l'article 3, paragraphe 2.**
3. **Une** injonction européenne de production **visant à obtenir** des données relatives aux abonnés ou **des adresses IP aux seules fins de la détermination de l'identité de personnes précises ayant un lien direct avec les procédures explicitement visées à l'article 3, paragraphe 2,** peut être émise pour toutes les infractions pénales.
4. **Une** injonction européenne de production de données relatives **au trafic** ou de données relatives au contenu ne peut être émise **que pour toutes les infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins 3 ans.**
- 4 bis. **Les injonctions européennes de production de données relatives au trafic ou de données relatives au contenu peuvent également être émises pour les infractions suivantes:**
 - a) **pour les infractions suivantes, si elles sont totalement ou partiellement commises au moyen d'un système d'information:**
 - les infractions définies aux articles 3, 4 et 5 de la décision-cadre 2001/413/JAI du Conseil;
 - les infractions définies aux articles 3 à 8 de la directive 2013/40/UE;
 - b) **pour les infractions pénales définies aux articles 3 à 12 et 14 de la directive (UE) 2017/541;**
 - b bis) **pour les infractions pénales définies aux articles 3 à 7 de la directive 2011/93/UE.**
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; **dans le cas des données relatives au trafic et au contenu, et lorsque l'État d'émission est soumis à une procédure visée à l'article 7, paragraphe 1 ou paragraphe 2, du traité UE, les informations relatives à la procédure spéciale visée à l'article 9, paragraphe 2 bis, du présent règlement;**
 - b) **les destinataires** de l'injonction européenne de production visés à l'article 7;

- c) *les personnes individuellement identifiables ou*, si l'injonction a pour unique but d'identifier une personne, *tout autre identifiant unique tel que le nom d'utilisateur ou l'identifiant de connexion*;
- d) la catégorie de données requises (données relatives aux abonnés, données relatives *au trafic* ou données relatives au contenu);
- e) la durée pour laquelle la production est requise, *adaptée autant que possible*;
- f) les dispositions applicables du droit pénal de l'État d'émission;
- g) en cas d'urgence, les raisons *dûment justifiées* de cette divulgation;
- h) ■
- i) les motifs de la nécessité et de la proportionnalité de la mesure, *en tenant dûment compte des répercussions de la mesure sur les droits fondamentaux des personnes précises dont les données sont recherchées, ainsi que de la gravité de l'infraction*.

6. ■

7. Si l'autorité d'émission a des raisons de croire que les données requises sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre du fournisseur de services destinataire *ou de l'État membre où la personne dont les données sont demandées réside ou est liée par une obligation de secret professionnel ou de confidentialité des communications*, 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 *demande* des éclaircissements avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État membre concerné, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen *en matière pénale*. *Lorsque* l'autorité d'émission constate que les données demandées sont protégées par ces immunités et privilèges, ou que leur divulgation porterait atteinte aux intérêts fondamentaux de l'autre État membre, *l'autorité d'émission* n'émet pas l'injonction européenne de production.

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.
2. Elle 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, *compte tenu des droits de la personne concernée*. Les injonctions européennes de conservation de données peuvent être émises pour toutes les infractions pénales, *si elles auraient pu être*

demandées sous les mêmes conditions dans une affaire nationale similaire dans l'État d'émission, lorsqu'il existe des raisons suffisantes pour penser qu'une infraction pénale a été commise, qu'elle est suffisamment grave pour justifier la conservation transfrontière des données et que les informations demandées sont pertinentes pour l'enquête. Elle se limite aux données des personnes précises ayant un lien direct avec les procédures explicitement visées à l'article 3, paragraphe 2.

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) les destinataires de l'injonction européenne de conservation visés à l'article 7;
 - c) les personnes *individuellement identifiables* dont les données sont conservées *ou*, si l'injonction a pour unique but d'identifier une personne, *tout autre identifiant unique tel que le nom d'utilisateur ou l'identifiant de connexion*;
 - d) la catégorie de données devant être conservée (données relatives aux abonnés, données relatives *au trafic* ou données relatives au contenu);
 - e) la durée pour laquelle la conservation est requise, *adaptée autant que possible*;
 - 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, *en tenant dûment compte des répercussions de la mesure sur les droits fondamentaux des personnes précises dont les données sont recherchées, ainsi que de la gravité de l'infraction.*
- 3 bis. *Si l'autorité d'émission a des raisons de croire que les données requises sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre du fournisseur de services destinataire ou que leur conservation peut porter atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales, l'autorité d'émission doit demander des éclaircissements avant d'émettre l'injonction européenne de conservation, notamment en consultant les autorités compétentes de l'État membre concerné, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. Lorsque l'autorité d'émission constate que les données demandées sont protégées par ces immunités et privilèges, ou que leur conservation porterait atteinte aux intérêts fondamentaux de l'autre État membre, elle n'émet pas l'injonction européenne de production.*

Article 6 bis

Représentant légal

1. *Les fournisseurs de services qui offrent des services dans les États membres soumis au présent règlement, mais ne sont pas établis dans l'Union, désignent un représentant légal pour la réception, le respect et l'exécution des injonctions européennes de production et des injonctions européennes de conservation émises*

par les autorités compétentes des États membres, aux fins de la collecte d'informations électroniques dans le cadre d'une procédure pénale. Le représentant légal est établi dans un des États membres (soumis au présent règlement) où le fournisseur de services offre ses services.

- 2. Les fournisseurs de services qui offrent des services dans les États membres soumis au présent règlement, mais sont établis dans un État membre non soumis au présent règlement, désignent un représentant légal pour la réception, le respect et l'exécution des injonctions européennes de production et des injonctions européennes de conservation émises par les autorités compétentes des États membres, aux fins de la collecte d'informations électroniques dans le cadre d'une procédure pénale. Le représentant légal est établi dans l'un des États membres soumis au présent règlement où le fournisseur de services offre ses services.*
- 3. Les prestataires de services qui font partie d'un groupe sont autorisés à désigner collectivement un seul représentant légal.*
- 4. Le représentant légal est chargé de la réception, du respect et de l'exécution de ces décisions et injonctions pour le compte du prestataire de services concerné.*
- 5. Lorsque les fournisseurs de services désignent un représentant légal, ils notifient par écrit l'État membre du lieu d'établissement de celui-ci. La notification contient la désignation et les coordonnées de son représentant légal, ainsi que toutes les modifications s'y rapportant.*
- 6. La notification précise la ou les langues officielles de l'Union, visées dans le règlement n° 1/58, dans lesquelles il est possible de s'adresser au représentant légal. Celles-ci comprennent au moins une des langues acceptées par l'État membre dans lequel le représentant légal est établi.*
- 7. Les informations notifiées aux États membres conformément au présent article sont mises à disposition sur une page internet dédiée du réseau judiciaire européen. Ces informations sont régulièrement mises à jour.*
- 8. Les États membres veillent à ce que le représentant légal désigné puisse être considéré comme responsable du non-respect d'obligations au titre du présent règlement, sans préjudice de la responsabilité du prestataire de services et des actions en justice qui pourraient être intentées contre ce dernier.*
- 9. Les États membres déterminent le régime des sanctions applicables aux violations du présent article et prennent toutes les mesures nécessaires pour garantir la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives.*

Article 7

Destinataires d'une injonction européenne de production et d'une injonction européenne de conservation

1. *Aux fins de la collecte d'informations électroniques dans le cadre d'une procédure pénale, l'injonction européenne de production et l'injonction européenne de conservation sont adressées directement et simultanément:*
 - a) *à l'établissement principal du fournisseur de services ou, le cas échéant, à son représentant légal dans l'État d'exécution, désigné par le fournisseur de services aux fins de la collecte de preuves dans le cadre d'une procédure pénale; et*
 - b) *à l'autorité d'exécution.*
- 1 bis. *Les États membres veillent à ce que tout fournisseur de services établi sur leur territoire informe cet État membre par écrit du lieu de son établissement principal. La notification contient les coordonnées, ainsi que toutes les modifications s'y rapportant.*
- 1 ter. *Les informations notifiées aux États membres conformément au paragraphe 1 bis sont mises à disposition sur une page internet dédiée du réseau judiciaire européen. Ces informations sont régulièrement mises à jour.*
2. █
3. █
4. █

Article 7 bis

Système européen commun d'échange

1. *D'ici au ... [date de mise en application du présent règlement], la Commission établit un système européen commun d'échange comportant des canaux sécurisés de traitement des communications, authentifications et transmissions transfrontières autorisées des injonctions et des données demandées entre les autorités compétentes et les fournisseurs de services. Les autorités compétentes et les fournisseurs de services utilisent ce système aux fins du présent règlement.*
2. *La Commission veille à ce que le système garantisse un échange effectif, fiable et fluide des informations, ainsi qu'un niveau élevé de sécurité, de confidentialité et d'intégrité, de même que la nécessaire protection de la vie privée et les données à caractère personnel, conformément au règlement (UE) 2018/1725, au règlement (UE) 2016/679, à la directive (UE) 2016/680, et à la directive 2002/58/CE. À cette fin, des technologies de pointe, ouvertes et couramment utilisées en matière de signature électronique et de chiffrement sont appliquées.*
3. *Lorsque les fournisseurs de services ou les États membres ont déjà mis en place des systèmes spécifiques ou d'autres canaux sécurisés pour le traitement des demandes de données à des fins répressives, il est possible de connecter ces systèmes ou canaux au système européen commun d'échange numérique.*

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 aux destinataires tels que définis à l'article 7 **via le système défini à l'article 7 bis** 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 sont transmis directement **via le système défini à l'article 7 bis**, permettant aux destinataires de produire une trace écrite et permettant aux destinataires d'établir **l'authenticité de l'injonction et de l'autorité d'émission**.
3. L'EPOC contient **toutes** les informations énumérées à l'article 5, paragraphe 5, points a) à **i**), y compris des informations suffisantes pour permettre aux destinataires d'identifier et de contacter l'autorité d'émission, **et les informations concernant les moyens et les interfaces techniques qu'elle a à sa disposition pour recevoir les données produites ou l'emplacement de ces informations**.
4. L'EPOC-PR contient **toutes** les informations énumérées à l'article 6, paragraphe 3, points a) à **g**), y compris des informations suffisantes pour permettre aux destinataires d'identifier et de contacter l'autorité d'émission.
5. S'il y a lieu, l'EPOC ou l'EPOC-PR est traduit dans une langue officielle **de l'État d'exécution ou dans toute autre langue explicitement acceptée par celui-ci conformément au paragraphe 5 bis**.

Article 8 bis

Exécution d'un EPOC concernant les données relatives aux abonnés et les adresses IP dans le seul but d'identifier une personne

1. **Un EPOC concernant les données relatives aux abonnés ou les adresses IP, dans le seul but d'identifier une personne, est adressé directement et simultanément:**
 - a) **à l'établissement principal du fournisseur de services ou, le cas échéant, là où son représentant légal est établi; et**
 - b) **à l'autorité d'exécution.**

L'information simultanée de l'autorité d'exécution n'a pas d'effet suspensif sur les obligations du fournisseur de services conformément au paragraphe 1.

- 2. Dès réception d'un EPOC concernant les données relatives aux abonnés ou les adresses IP dans le seul but d'identifier une personne, le fournisseur de services veille à ce que les données demandées soient transmises directement à l'autorité d'émission indiquée dans l'EPOC, dès que possible et au plus tard et dans les 10 jours suivant la réception de l'EPOC. Lorsqu'il transmet les données demandées, le fournisseur de services envoie simultanément, pour information, une copie des données transférées à l'autorité d'exécution.*
- 3. Dans les cas d'urgence, le fournisseur de services transmet les données requises sans retard injustifié au plus tard 16 heures après la réception de l'EPOC. Lorsqu'il transmet les données demandées, le fournisseur de services les met simultanément à la disposition de l'autorité d'exécution pour information.*
- 4. Lorsque l'autorité d'exécution décide d'invoquer l'un des motifs énumérés à l'article 10 bis, paragraphe 1, elle agit dès que possible et au plus tard dans les délais visés aux paragraphes 2 ou 3, et elle informe immédiatement l'autorité d'émission et le fournisseur de services de sa décision. L'autorité d'émission efface les données. Lorsque les données demandées n'ont pas encore été transmises à l'autorité d'émission, le fournisseur de services destinataire ne transmet pas les données.*
- 5. Si l'EPOC est incomplet, contient des erreurs manifestes, sur le fond ou sur la forme, ou ne contient pas suffisamment d'informations pour son exécution, le fournisseur de services en informe sans retard injustifié l'autorité d'émission et l'autorité d'exécution indiquées dans l'EPOC et demande des éclaircissements ou, si besoin, des corrections de la part de l'autorité d'émission 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. Les délais prévus aux paragraphes 2 et 3 ne s'appliquent qu'après la fourniture d'éclaircissements. En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.*
- 6. Si le fournisseur de services ne peut pas respecter ses obligations pour cause de force majeure ou d'impossibilité de fait en raison de circonstances qui ne lui sont pas imputables, notamment parce que la personne dont les données sont requises n'est pas son client, ou que les données ont été supprimées avant la réception de l'EPOC, le fournisseur de services 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. Si les conditions pertinentes sont remplies, l'autorité d'émission retire l'EPOC et en informe les destinataires.*
- 7. Dans tous les cas où le fournisseur de services ne fournit pas les informations requises ou ne les fournit pas de manière exhaustive ou dans les délais, pour d'autres raisons, y compris techniques ou opérationnelles, il en informe l'autorité d'émission et l'autorité d'exécution mentionnées dans l'EPOC sans délai injustifié*

et au plus tard dans les délais prévus aux paragraphes 2 et 3 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 les destinataires. Si le fournisseur de services estime que l'EPOC ne peut pas être exécuté parce qu'il apparaît, sur la base des seules informations contenues dans l'EPOC, que celui-ci est manifestement abusif ou qu'il dépasse la finalité de l'injonction, le fournisseur de services envoie également le formulaire figurant à l'annexe III à l'autorité d'émission ainsi qu'à l'autorité d'exécution figurant dans l'EPOC, avec un effet suspensif en ce qui concerne la transmission des données requises. Dans ce cas, l'autorité d'exécution peut demander des éclaircissements à l'autorité d'émission concernant l'injonction européenne de production, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Les délais prévus aux paragraphes 2 et 3 ne s'appliquent qu'après la fourniture d'éclaircissements. En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.

8. *Lorsque le fournisseur de services ne fournit pas immédiatement les données demandées, conformément aux paragraphes 3, 4 et 5, il conserve, dans la mesure du possible, les données demandées. Les données sont conservées jusqu'à leur production ou jusqu'à ce que l'EPOC soit retiré ou considéré comme nul et non avenue.*

Article 9

Exécution d'un EPOC concernant des données relatives au trafic ou au contenu

- 1 bis. *Un EPOC concernant des données relatives au trafic ou au contenu est adressé directement et simultanément:*

a) à l'établissement principal du fournisseur de services ou, le cas échéant, là où son représentant légal est établi; et

b) à l'autorité d'exécution.

1. *Dès réception de l'EPOC concernant les données relatives au trafic et aux contenus, le fournisseur de services agit rapidement pour conserver les données.*

- 1 bis. *Lorsque l'autorité d'exécution décide de refuser l'EPOC sur la base de l'un des motifs énumérés à l'article 10 bis, elle agit dès que possible et au plus tard dans les 10 jours à compter de la réception de l'EPOC, et elle informe immédiatement l'autorité d'émission et le fournisseur de services de sa décision.*

2. *Dans les cas d'urgence, lorsque l'autorité d'exécution décide de refuser l'EPOC sur la base de l'un des motifs énumérés à l'article 10 bis, elle agit dès que possible et au plus tard 16 heures après la réception de l'EPOC, et elle informe immédiatement l'autorité d'émission et le fournisseur de services de sa décision.*

- 2 bis.** *Lorsque l'État d'émission fait l'objet d'une procédure visée à l'article 7, paragraphe 1 ou paragraphe 2, du traité sur l'Union européenne, le fournisseur de services ne transmet les données demandées qu'après en avoir reçu l'autorisation écrite explicite de la part de l'autorité d'exécution. À cet effet, l'autorité d'exécution évalue l'injonction de l'autorité d'émission avec toute la diligence requise et vérifie en particulier les motifs de non-reconnaissance et de non-exécution conformément à l'article 10 bis, avant de donner son approbation écrite dans les délais fixés aux paragraphes 1 bis et 2.*
- 2 ter.** *Sans préjudice du paragraphe 2 bis, si l'autorité d'exécution n'a invoqué aucun des motifs énumérés à l'article 10 bis dans les délais fixés aux paragraphes 1 bis et 2, le fournisseur de services auquel l'injonction est adressée s'assure que les données demandées soient immédiatement et directement transmises à l'autorité d'émission ou aux autorités répressives comme indiqué dans l'EPOC.*
- 2 quater.** *Lorsque, dans un cas donné, il n'est pas possible à l'autorité d'exécution de respecter le délai fixé aux paragraphes 1 ou 2, elle informe sans tarder l'autorité d'émission et le fournisseur de services par tout moyen, en indiquant les raisons du retard et une estimation du temps qu'il faudra pour y remédier.*
3. Si l'EPOC est incomplet, contient des erreurs manifestes, **sur le fond ou sur la forme**, ou ne contient pas suffisamment d'informations pour son exécution, le **fournisseur de services** en informe l'autorité d'émission **et l'autorité d'exécution** indiquées dans l'EPOC sans retard injustifié et demande des éclaircissements **ou, si besoin, des corrections de la part de l'autorité d'émission** 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. Les délais prévus aux paragraphes 1 **bis** et 2 ne s'appliquent qu'après la fourniture d'éclaircissements. **En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.**
4. Si le **fournisseur de services** ne peut pas respecter ses obligations pour cause de force majeure ou d'impossibilité de fait **en raison de circonstances** qui ne lui **sont** pas imputables, notamment parce que la personne dont les données sont requises n'est pas leur client, ou que les données ont été supprimées avant la réception de l'EPOC, le **fournisseur de services** en informe l'autorité d'émission **ainsi que l'autorité d'exécution** mentionnées dans l'EPOC sans retard injustifié, en expliquant les raisons au moyen du formulaire figurant à l'annexe III. Si les conditions pertinentes sont remplies, l'autorité d'émission retire l'EPOC **et en informe les destinataires.**
5. Dans tous les cas où le **fournisseur de services** ne fournit pas les informations requises ou ne les fournit pas de manière exhaustive ou dans les délais, pour d'autres raisons, **y compris techniques ou opérationnelles**, il en informe l'autorité d'émission **et l'autorité d'exécution mentionnées dans l'EPOC** sans délai injustifié et au plus tard dans les délais prévus aux paragraphes 1 **bis** 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 *les destinataires*.

Si le *fournisseur de services* estime que l'EPOC ne peut pas être exécuté parce qu'il apparaît, sur la base des seules informations contenues dans l'EPOC, que celui-ci est manifestement abusif *ou qu'il dépasse la finalité de l'injonction*, le *fournisseur de services* envoie également le formulaire figurant à l'annexe III à l'autorité *d'émission ainsi qu'à l'autorité d'exécution mentionnées dans l'EPOC, avec un effet suspensif en ce qui concerne la transmission des données requises*. Dans ce cas, l'autorité *d'exécution* compétente peut demander des éclaircissements à l'autorité d'émission concernant l'injonction européenne de production, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. *L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Les délais prévus aux paragraphes 1 bis et 2 ne s'appliquent qu'après la fourniture d'éclaircissements. En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.*

6. *Au cours des procédures visées aux paragraphes 1, 1 bis, 2, 2 ter, 2 quater, 3, 4 et 5, le fournisseur de services conserve les données requises si possible. Les données sont conservées jusqu'à leur production ou jusqu'à ce que l'EPOC soit retiré ou considéré comme nul et non avenue.*

Article 10

Exécution d'un EPOC-PR

- 1 bis. Un EPOC-PR est adressé directement et simultanément:

a) à l'établissement principal du fournisseur de services ou, le cas échéant, là où son représentant légal est établi; et

b) à l'autorité d'exécution.

L'information simultanée de l'autorité d'exécution n'a pas d'effet suspensif sur les obligations du fournisseur de services en vertu du paragraphe 1.

1. Dès réception de l'EPOC-PR, le fournisseur de services *agit rapidement pour conserver* les données requises. La conservation prend fin après 60 jours, à moins que l'autorité d'émission ne confirme que la demande de production suivante a été introduite. *L'EPOC-PR peut être prolongé de 30 jours, uniquement lorsque cela est nécessaire pour permettre une évaluation supplémentaire de la pertinence des données.*
2. Si l'autorité d'émission *transmet l'injonction européenne de production suivante* dans le délai fixé au paragraphe 1, le *fournisseur de services* conserve les données aussi longtemps que nécessaire pour *pouvoir exécuter l'injonction européenne de production conformément aux articles 8 bis ou 9.*
3. Si la conservation n'est plus nécessaire, l'autorité d'émission en informe les destinataires sans retard injustifié *et la conservation cesse immédiatement.*

4. Si l'EPOC-PR est incomplet, contient des erreurs manifestes, **sur le fond ou sur la forme**, ou ne contient pas suffisamment d'informations pour son exécution, le **fournisseur de services** en informe l'autorité d'émission **et l'autorité d'exécution** indiquées dans l'EPOC-PR sans retard injustifié et demande des éclaircissements **ou, si besoin, des corrections de la part de l'autorité d'émission** 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. Les destinataires **veillent** à obtenir les éclaircissements nécessaires pour permettre **au fournisseur de services** de remplir les obligations énoncées aux paragraphes **1, 2 et 3**. **En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.**
5. Si le **fournisseur de services** ne peut pas respecter **ses obligations** pour cause de force majeure ou d'impossibilité de fait **en raison de circonstances** qui ne lui **sont** pas imputables, notamment parce que la personne dont les données sont requises n'est pas leur client, ou que les données ont été supprimées avant la réception de l'**EPOC-PR**, le **fournisseur de services** prend contact avec l'autorité d'émission **et l'autorité d'exécution** figurant dans l'EPOC-PR sans retard injustifié, en expliquant les raisons, au moyen du formulaire figurant à l'annexe III. Si **les conditions pertinentes** sont remplies, l'autorité d'émission retire l'EPOC-PR **et en informe les destinataires**.
6. Dans tous les cas où le **fournisseur de services** ne conserve pas les informations requises, pour d'autres raisons énumérées dans le formulaire de l'annexe III, **y compris pour des raisons opérationnelles ou techniques**, il en informe l'autorité d'émission **et l'autorité d'exécution figurant dans l'EPOC-PR** 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.

Si le fournisseur de services estime que l'EPOC-PR ne peut pas être exécuté parce qu'il apparaît, sur la base des seules informations contenues dans l'EPOC-PR, que celui-ci est manifestement abusif ou qu'il dépasse la finalité de l'injonction, le fournisseur de services envoie également le formulaire figurant à l'annexe III à l'autorité d'émission ainsi qu'à l'autorité d'exécution figurant dans l'EPOC-PR. Dans ce cas, l'autorité d'exécution compétente peut demander des éclaircissements à l'autorité d'émission concernant l'injonction européenne de conservation, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Le délai prévu au paragraphe 1 ne s'applique qu'après la fourniture d'éclaircissements. En l'absence de réaction de la part de l'autorité d'émission, l'injonction est considérée comme nulle et non avenue.

Article 10 bis
Motifs de non-reconnaissance ou de non-exécution

1. *Sans préjudice de l'article 1^{er}, paragraphe 2, au moment de l'évaluation de l'EPOC par l'autorité d'exécution, celle-ci refuse l'EPOC dans les cas suivants:*
 - a) *les conditions pour émettre une injonction européenne de production, telles qu'elles sont établies à l'article 5 du présent règlement, ne sont pas remplies;*
 - b) *l'exécution de l'injonction européenne de production serait contraire au principe de non bis in idem;*
 - c) *il existe des motifs sérieux de croire que l'exécution de l'injonction européenne de production serait incompatible avec les obligations de l'État membre au titre de l'article 6 du traité UE et de la charte; ou*
 - d) *il existe une immunité, un privilège ou des règles relatives à la détermination et à la restriction de la responsabilité pénale en matière de liberté de la presse et de liberté d'expression dans d'autres médias en vertu du droit de l'État d'exécution, qui rendent impossible l'exécution de l'injonction européenne de production.*

2. *En sus des cas visés au paragraphe 1, l'EPOC concernant les données relatives au trafic et aux contenus peut être refusé par l'autorité d'exécution dans les cas suivants:*
 - a) *l'injonction européenne de production porterait préjudice à des intérêts nationaux fondamentaux en matière de sécurité, mettrait en péril la source des informations ou impliquerait l'utilisation d'informations classifiées relatives à des activités de renseignement spécifiques;*
 - b) *l'injonction européenne de production concerne une infraction pénale qui est supposée avoir été commise en dehors du territoire de l'État d'émission et, en tout ou en partie, sur le territoire de l'État d'exécution, et les faits pour lesquels l'EPOC a été émis ne constituent pas une infraction pénale selon le droit de l'État d'exécution;*
 - c) *les faits pour lesquels l'EPOC a été émis ne constituent pas une infraction au titre du droit de l'État d'exécution, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions énumérées à l'annexe III bis, conformément à ce qui a été indiqué par l'autorité d'émission dans l'EPOC, si ces faits sont passibles dans l'État d'émission d'une peine ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins trois ans;*

- d) *l'exécution de l'injonction européenne de production est limitée en vertu du droit de l'État d'exécution à une liste ou à une catégorie d'infractions ou à des infractions passibles de sanctions plus lourdes; ou*
- e) *le respect de l'injonction européenne de production entraverait la législation d'un pays tiers interdisant la divulgation des données concernées.*
3. *Le point e) du paragraphe 2 s'applique conformément à la procédure prévue à l'article 14 bis.*
4. *Lorsque l'injonction européenne de production concerne une infraction en matière de taxes ou d'impôts, de douane et de change, l'autorité d'exécution ne peut refuser la reconnaissance ou l'exécution au motif que le droit de l'État d'exécution n'impose pas le même type de taxe ou de droits ou ne contient pas le même type de réglementation en matière de taxes, d'impôts, de douane ou de change que le droit de l'État d'émission.*
5. *Dans les cas visés aux paragraphes 1 et 2 du présent article, avant de décider de ne pas reconnaître ou de ne pas exécuter une injonction européenne de production, en tout ou partie, l'autorité d'exécution consulte l'autorité d'émission par tout moyen approprié et, s'il y a lieu, demande à l'autorité d'émission de fournir toutes les informations nécessaires sans délai.*
6. *Dans le cas visé au paragraphe 1, point d), et lorsque la levée du privilège ou de l'immunité relève de la compétence d'une autorité de l'État d'exécution, l'autorité d'exécution lui demande d'exercer cette compétence immédiatement. Lorsque la levée du privilège ou de l'immunité relève de la compétence d'une autorité d'un autre État membre ou d'une organisation internationale, il revient à l'autorité d'émission de demander à l'autorité concernée d'exercer cette compétence.*
7. *L'autorité d'exécution qui fait prévaloir l'un des motifs de non-reconnaissance ou de non-exécution énumérés aux paragraphes 1 et 2 du présent article en informe l'autorité d'émission au moyen du formulaire figurant l'annexe III.*

Article 11

Information de l'utilisateur *et confidentialité*

1. *Le fournisseur de services informe sans retard injustifié la personne dont les données sont requises. Le fournisseur de services prend les mesures opérationnelles et techniques nécessaires les plus modernes afin de garantir la confidentialité, le secret et l'intégrité de l'EPOC ou de l'EPOC-PR ainsi que des données produites ou conservées.*
- 1 bis. *Aussi longtemps qu'elle le juge nécessaire et proportionné pour éviter d'entraver la procédure pénale concernée ou pour protéger les droits fondamentaux d'une autre personne, et en tenant dûment compte de l'incidence de la mesure sur les droits*

fondamentaux de la personne dont les données sont demandées, l'autorité d'émission peut demander au fournisseur de services de s'abstenir d'informer la personne dont les données sont demandées, sur la base d'une injonction judiciaire. Cette injonction est dûment justifiée, précise la durée de l'obligation de confidentialité et fait l'objet d'un réexamen périodique.

2. Si l'autorité d'émission a demandé aux destinataires, *en s'appuyant sur une décision de justice*, de s'abstenir d'informer la personne dont les données sont requises, elle informe sans retard injustifié la personne dont les données sont requises par l'EPOC ou l'EPOC-PR au sujet de la production *ou de la conservation* des données. Cette information peut être retardée aussi longtemps que nécessaire et proportionné pour éviter d'entraver la procédure pénale afférente, *compte tenu des droits du suspect et de la personne poursuivie, sans préjudice des droits de la défense et de l'existence de voies de recours effectives.*
3. Lorsqu'elle informe la personne, l'autorité d'émission fournit des informations sur tous les recours disponibles visés à l'article 17.

*Article 11 bis
Restrictions de l'utilisation des informations obtenues*

Les informations électroniques obtenues conformément au présent règlement ne sont pas utilisées aux fins de procédures autres que celles pour lesquelles elles ont été obtenues conformément au présent règlement, sauf en cas de menace imminente pour la vie ou l'intégrité physique d'une personne.

*Article 11 ter
Suppression des informations électroniques*

1. *Les informations électroniques recueillies en violation du présent règlement sont effacées sans délai.*
2. *Les informations électroniques qui ne sont plus nécessaires à toutes les phases de la procédure pour lesquelles elles ont été produites ou conservées, y compris aux éventuels recours, sont immédiatement effacées également, à moins que cela n'affecte les droits de la défense de la personne suspectée ou poursuivie. Des réexamens périodiques de la nécessité de stocker les informations électroniques sont prévus.*
3. *La personne dont les données ont été demandées est informée de l'effacement des données sans retard injustifié.*

Article 11 quater

Admissibilité des informations électroniques dans les procédures judiciaires

Les informations électroniques obtenues en violation du présent règlement, y compris lorsque les critères établis dans le présent règlement ne sont pas remplis, sont irrecevables devant une juridiction. Lorsque des informations électroniques ont été obtenues avant

qu'un motif de non-reconnaissance énuméré à l'article 10 bis (nouveau) du règlement n'ait été invoqué, celles-ci sont également irrecevables devant une juridiction.

Article 12

Remboursement des frais

Lorsque le fournisseur de services le réclame, l'État d'émission rembourse les coûts justifiés supportés par le fournisseur et liés à l'exécution de l'injonction européenne de production ou l'injonction européenne de conservation. Pour des raisons pratiques, le fournisseur de services peut demander le remboursement des frais à l'État d'exécution. Lorsque le fournisseur de services choisit l'État d'exécution, l'État d'émission rembourse ces frais à l'État d'exécution. Les États membres communiquent les règles de remboursement à la Commission, qui les rend publiques.

Chapitre 3: Sanctions, *procédure de réexamen* et *voies de recours*

Article 13

Sanctions

1. *Les États membres fixent les règles relatives aux sanctions applicables aux violations des obligations prévues aux articles 8 bis, 9, 10 et 11 du présent règlement en ce qui concerne les fournisseurs de services sur leur territoire et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Les sanctions prévues par les législations nationales des États membres sont effectives, proportionnées et dissuasives. Les États membres notifient sans délai ces règles et mesures à la Commission et l'informent sans tarder de toute modification ultérieure les concernant.*
- 1 bis. Sans préjudice de leurs obligations en matière de protection des données, les fournisseurs de services ne sont pas tenus responsables dans les États membres des conséquences résultant de la conformité à un EPOC ou un EPOC-PR.*

Article 14

Procédure de mise en œuvre

1. Si le *fournisseur de services* ne respecte pas un EPOC dans les délais ou un EPOC-PR sans fournir de raisons *et si l'autorité d'exécution n'a invoqué aucun des motifs de non-reconnaissance ou de non-exécution énumérés à l'article 10 bis*, l'autorité d'émission peut *demander* à l'autorité compétente de l'État *d'exécution d'exécuter*

l'injonction européenne de production accompagnée ou l'injonction européenne de conservation ■ .

2. ■
3. ■ L'autorité *d'exécution* enjoint formellement au *fournisseur de services* de se conformer à l'obligation en question, informe ce dernier de la possibilité de s'opposer à l'*exécution* en invoquant les motifs énumérés aux *articles 8 bis, 9 et 10*, 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. ■
5. ■
6. En cas d'objection du *fournisseur de services*, l'autorité *d'exécution* décide de mettre en œuvre *ou de ne pas reconnaître* l'injonction sur la base des informations fournies par le *fournisseur de services* et, si nécessaire, des informations supplémentaires obtenues auprès de l'autorité d'émission. *L'autorité d'exécution notifie sans retard injustifié sa décision au service et à l'autorité d'émission.*
7. ■
8. ■
9. Si l'autorité *d'exécution* obtient les données du *fournisseur de services*, elle les transmet à l'autorité d'émission sans retard injustifié.
10. Si le *fournisseur de services* ne respecte pas ses obligations, l'autorité *d'exécution* inflige une sanction conformément à l'*article 13*. Un recours juridictionnel effectif est disponible contre la décision d'infliger une amende.

Article 14 bis

Procédure de réexamen en cas d'obligations entrant en conflit avec le droit d'un pays tiers

1. *Lorsque le fournisseur de services ou l'autorité d'exécution estime que le respect de l'injonction européenne de production ou de l'injonction européenne de conservation conduirait à enfreindre la législation en vigueur d'un pays tiers qui interdit la divulgation des données concernées, il en informe l'autorité d'émission et les destinataires concernés sans délai et au plus tard dans les 10 jours suivant la réception de l'injonction. Dans ce cas, l'exécution de l'injonction est suspendue.*
2. *Cette notification comprend tous les détails pertinents sur la loi du pays tiers, son applicabilité à l'affaire en question et la nature de l'obligation contradictoire.*
3. *L'autorité compétente de l'État d'émission examine l'injonction européenne de production ou l'injonction européenne de conservation et informe les destinataires, dans les 10 jours suivant la réception de la notification, sur la base des critères suivants:*

- a) *les intérêts protégés 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 à la juridiction de l'État d'émission et au pays tiers, comme l'indiquent entre autres:*
 - i) *la localisation, la nationalité et le lieu de résidence de la personne dont les données sont requises et/ou de la ou des victimes;*
 - ii) *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;*
 - d) *les intérêts de l'État d'émission à obtenir les informations électroniques concernées, en fonction de la gravité de l'infraction et de l'importance d'obtenir rapidement des informations électroniques;*
 - e) *les éventuelles conséquences pour les destinataires s'ils se conforment à l'injonction européenne de production ou à l'injonction européenne de conservation, y compris les sanctions qui peuvent être encourues par les fournisseurs de services au titre du droit du pays tiers.*
4. *Dans les 10 jours suivant la réception de la notification, l'autorité retire, maintient ou adapte l'injonction, s'il y a lieu, pour appliquer ces critères. À cette fin, l'autorité d'émission peut solliciter des éclaircissements sur la législation applicable du pays tiers, conformément à la directive (UE) 2016/680, dans la mesure où cela n'entrave pas les délais prévus par le présent règlement. En cas de retrait, l'autorité d'émission en informe immédiatement les destinataires.*
5. *Lorsque l'autorité d'émission décide de maintenir l'injonction, elle en informe les destinataires. Tout en tenant dûment compte de la décision de l'autorité d'émission et après avoir également consulté l'autorité compétente du pays tiers, conformément à la directive (UE) 2016/680, dans la mesure où cela ne fait pas obstacle au respect des délais prévus par le présent règlement, l'autorité d'exécution prend, dans les 10 jours suivant la réception de la décision de l'autorité d'émission, une décision finale sur la base des critères énumérés au paragraphe 3 et informe l'autorité d'émission, le fournisseur de services et l'autorité compétente du pays tiers de sa décision finale.*
6. *Pendant la durée de la procédure visée à l'article 14 bis, le fournisseur de services conserve les données demandées.*

Article 15



Article 16



Article 17

Recours effectifs

1. *Les personnes* dont les données ont été *demandées* au moyen d'une injonction européenne de production *ou d'une injonction européenne de conservation* ont droit à des recours effectifs contre *lesdites injonctions*, 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 *ou de l'État d'exécution conformément à la législation nationale* et comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité.
- 3 bis. *Les raisons de fond qui ont conduit à l'émission d'une injonction européenne de production ou d'une injonction européenne de conservation peuvent être contestées dans l'État d'émission, sans préjudice des garanties des droits fondamentaux dans l'État d'exécution.*
4. Sans préjudice de l'article 11, l'autorité d'émission *et l'autorité d'exécution prennent* les mesures appropriées pour veiller à ce que des informations sur les possibilités de recours *légaux* prévues par la législation nationale soient fournies *en temps utile, notamment pour déterminer à quel moment ces recours peuvent être exercés*, 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. █

Article 18



Chapitre 5: Dispositions finales

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 *informations* nécessaires seront collectées. Il précise quelles mesures la Commission et les États membres doivent prendre pour collecter et analyser les données et autres *informations*.

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:
 - a) le nombre d'EPOC et d'EPOC-PR émis *selon le* type de données requises, les **█** *destinataires* et la situation (cas d'urgence ou non);
a bis) le nombre d'EPOC émis en vertu de dérogations pour les cas d'urgence, y compris des détails sur les circonstances et les résultats possibles;
a ter) le nombre d'EPOC et d'EPOC-PR émis en vertu de la faculté offerte à l'autorité d'émission par l'article 11, paragraphe 1 bis, de demander au fournisseur de services de s'abstenir d'informer la personne dont les données sont requises, y compris des informations sur les circonstances et d'éventuelles informations ultérieures, conformément à l'article 11, paragraphe 2;
 - b) le nombre d'EPOC *et EPOC-PR* remplis et non remplis *selon le* type de données requises, les **█** *destinataires* et la situation (cas d'urgence ou non);
b bis) le nombre d'EPOC refusés selon le type de données requises, les destinataires, la situation (cas d'urgence ou non) et le motif de non-reconnaissance ou de non-exécution invoqué;
 - c) pour les EPOC remplis, la durée moyenne pour l'obtention des données requises depuis le moment où l'EPOC est émis jusqu'au moment où il est obtenu, *selon le* type de données requises, les **█** *destinataires* et la situation (cas d'urgence ou non);
c bis) pour les EPOC-PR remplis, la durée moyenne de la procédure relative à l'EPOC concerné qui suit l'EPOC-PR, depuis le moment où l'EPOC-PR est émis jusqu'au moment où l'EPOC est émis, selon le type de données requises et les destinataires;
 - d) **█**;
 - e) le nombre de recours légaux formés contre les injonctions européennes de production *et les injonctions européennes de conservation* dans l'État d'émission et dans l'État *d'exécution* *selon le* type de données requises;
 - f) *les sanctions encourues, conformément à l'article 13, selon le type de données requises, les destinataires, la situation (cas d'urgence ou non) et le montant des sanctions;*

g) un aperçu des coûts réclamés par les fournisseurs de services liés à l'exécution de l'EPOC ou de l'EPOC-PR et des coûts remboursés par les autorités d'émission;

h) le nombre de procédures d'exécution engagées selon le type de données requises, les destinataires, la situation (cas d'urgence ou non) et le résultat final.

2 bis. La Commission publie, au plus tard le 30 juin de chaque année, un rapport contenant les données visées au paragraphe 2, sous forme de compilation comprenant une subdivision par État membre.

Article 20



Article 21



Article 22

Notifications

1. Le... *[12 mois avant la 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 et/ou valider des injonctions européennes de production et des injonctions européennes de conservation;

b) l'autorité *d'exécution* à laquelle *l'EPOC ou l'EPOC-PR est transmis en vue de l'exécution ou de la mise en œuvre des* injonctions européennes de production et *des* injonctions européennes de conservation;

b bis) lorsque des fournisseurs de services ou des États membres ont déjà mis en place des systèmes spécifiques ou d'autres canaux sécurisés pour le traitement de demandes de données présentées à des fins répressives, les moyens et les interfaces techniques dont les autorités compétentes disposent pour recevoir les données produites aux fins d'interconnexion avec le système visé à l'article 7 bis ou pour y accéder;

c)

1 bis. À cette même date, les fournisseurs de services ayant des établissements dans plus d'un État membre informent la Commission du lieu où se situe leur établissement principal dans l'Union.

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 *en matière pénale* visé à l'article 9 de la décision 2008/976/JAI du Conseil²¹.

Article 23

Rapport avec les décisions d'enquête européennes *et les procédures d'entraide judiciaire*

Les autorités des États membres peuvent continuer à émettre des décisions d'enquête européennes conformément à la directive 2014/41/UE, *ou à recourir aux procédures d'entraide judiciaire existantes* pour la collecte d'*informations électroniques*, qui relèveraient également du champ d'application du présent règlement.

Article 24

Évaluation

Le... [2 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 *notamment une estimation du nombre de cas dans lesquels la dérogation d'urgence prévue à l'article 9, paragraphe 2, et la dérogation au principe de l'information des utilisateurs prévue à l'article 11 ont été appliquées.* ■ Le rapport est accompagné d'*une évaluation du fonctionnement du système commun européen d'échange ainsi que d'une évaluation du fonctionnement du règlement au regard de la directive n° 2014/41/UE du Parlement européen et du Conseil.* 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 [18 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

²¹ Décision 2008/976/JAI du Conseil du 16 décembre 2008 relative au Réseau judiciaire européen (JO L 348 du 24.12.2008, p. 130)

Par le Parlement européen
Le président

Par le Conseil
Le président

ANNEXE I

CERTIFICAT D'INJONCTION EUROPÉENNE DE PRODUCTION (EPOC) CONCERNANT LA PRODUCTION **D'INFORMATIONS** ÉLECTRONIQUES

Conformément au règlement (UE)... ¹ **■** le certificat d'injonction européenne de production (EPOC) doit ***être adressé directement et simultanément au fournisseur de services (ou, s'il y a lieu, à son représentant légal) et à l'autorité d'exécution en vue de l'exécution*** de l'EPOC. Si les données ne sont pas produites, le destinataire doit, à la réception de l'EPOC, conserver les données demandées, à moins que les informations contenues dans l'EPOC ne permettent pas d'identifier ces données. La conservation est maintenue jusqu'à ce que les données soient produites ou jusqu'à ce que l'autorité d'émission ou, le cas échéant, l'autorité chargée de l'exécution indique qu'il n'est plus nécessaire de conserver ni de produire les données.

Les destinataires doivent prendre les mesures nécessaires pour assurer la confidentialité de l'EPOC, ainsi que des données produites ou conservées.

SECTION A:

État

d'émission:

.....

Remarque: les coordonnées de l'autorité d'émission doivent être fournies à la fin du formulaire (sections E et F)

Destinataires (veuillez cocher la case appropriée):

- **le fournisseur de services ou, le cas échéant, son représentant légal:**

- **l'autorité d'exécution**

SECTION B: Délais

Les données demandées doivent être produites (cochez la case appropriée et complétez le cas échéant):

dans un délai maximal de 10 jours, **dès lors que l'autorité d'exécution n'a invoqué aucun des motifs de non-reconnaissance ou de non-exécution;**

dans un délai maximal de **16 heures** en cas d'urgence, **dès lors que l'autorité d'exécution n'a invoqué aucun des motifs de non-reconnaissance ou de non-exécution;**

- une menace imminente pour la vie ou l'intégrité physique d'une personne. Justification:

■

SECTION C: **Informations à l'utilisateur**

Veuillez noter que (cochez le cas échéant):

le **fournisseur de services** doit s'abstenir d'informer la personne dont les données sont demandées **de l'existence de l'EPOC sur la base d'une injonction judiciaire. Justification:...**

SECTION D: **Informations** électroniques à produire

i) Le présent EPOC concerne (cochez la ou les cases appropriées):

des données relatives aux abonnés **■**:

le nom, l'adresse, la date de naissance et les coordonnées (adresse électronique, numéro de téléphone) de l'utilisateur/du titulaire de l'abonnement et d'autres informations pertinentes permettant de l'identifier

la date et l'heure du premier enregistrement, le type d'enregistrement, la copie du contrat, les moyens de vérification de l'identité utilisés au moment de l'enregistrement, des copies des documents fournis par l'abonné

[] le type de service, y compris l'identifiant (numéro de téléphone, numéro de carte SIM, adresse MAC) et l'appareil ou les appareils associés

des informations relatives au profil (nom d'utilisateur, photo de profil)

des données sur la validation de l'utilisation du service, comme une adresse électronique de substitution fournie par l'utilisateur/le titulaire de l'abonnement

des codes PUK

l'adresse IP, aux seules fins d'identification de l'utilisateur:

- adresse IP:

- les enregistrements/journaux des connexions IP à des fins d'identification

des données relatives au trafic :

a) pour la téléphonie (mobile):

les identifiants sortants (A) et entrants (B) (numéro de téléphone, IMSI, IMEI)

l'heure et la durée des connexions

les tentatives d'appel

l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion

le support/téléservice utilisé (par exemple UMTS, GPRS)

b) pour l'internet

les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur , identité du message]

l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion

le volume de données

c) pour l'hébergement:

les fichiers-journaux

les tickets

historique d'achats

- l'historique de rechargement du solde prépayé

des données relatives au contenu :

- listes de contacts

une boîte de messagerie (internet)

un stockage en ligne (données générées par l'utilisateur)

une page

un journal/une sauvegarde de messages

une messagerie vocale

un contenu de serveurs

une sauvegarde d'appareil

ii) ***Informations supplémentaires nécessaires à l'exécution de l'EPOC:***

adresse IP:.....

numéro de téléphone:.....

adresse électronique:.....

numéro IMEI:.....
adresse MAC:.....
personne(s) dont les données sont demandées:.....
nom du service:
autre:

iii) *Période* pour laquelle la production des données est demandée:
.....

iv) Veuillez noter que (cochez et complétez le cas échéant):

les données demandées ont été conservées conformément à une demande de conservation émise précédemment par..... (indiquez l'autorité et, le cas échéant, la date de transmission de la demande et son numéro de référence) et adressée à (indiquez *les destinataires* de la demande et, s'il est disponible, le numéro de référence attribué par le destinataire)

v) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC est émis ainsi que disposition juridique ou code applicable:
.....

Le présent EPOC est émis relativement à des données relatives *au trafic* et/ou au contenu, en rapport avec (cochez la ou les cases appropriées, le cas échéant):

une ou plusieurs infractions pénales passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans dans l'État d'émission;

une ou plusieurs des infractions suivantes commises intégralement ou partiellement au moyen d'un système informatique:

infraction(s) visée(s) aux articles 3, 4 et 5 de la décision-cadre 2001/413/JAI du Conseil;

infraction(s) visées aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil;

infraction(s) visées aux articles 3 à 8 de la directive 2013/40/UE du Parlement européen et du Conseil;

[] des infractions visées aux articles 3 à 12 et 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil.

vi) Veuillez noter que (cochez le cas échéant):

Les données demandées sont stockées ou traitées dans le cadre d'une infrastructure institutionnelle mise à la disposition d'une entreprise ou d'une entité autre qu'une personne physique par un fournisseur de services, et le présent EPOC est adressé audit fournisseur de services car il ne serait pas indiqué d'adresser des mesures d'instruction à ladite entreprise ou entité, notamment parce que cela pourrait compromettre l'enquête.

vii) Autres informations utiles:
.....

SECTION E: Coordonnées de l'autorité qui a émis l'EPOC

Type d'autorité qui a émis l'EPOC (cochez la case appropriée):

juge, juridiction ou juge d'instruction

procureur (pour les données relatives aux abonnés *et les adresses IP aux seules fins d'identification de personnes spécifiques*)

procureur (pour les données relatives *au trafic* et celles relatives au contenu) → veuillez compléter également la section F

toute autre autorité compétente désignée par l'État d'émission → veuillez compléter également la section F

Coordonnées de l'autorité d'émission et/ou de son représentant certifiant que le contenu de l'EPOC est exact et correct:

Nom de l'autorité:.....

Nom de son représentant:.....

Fonction (titre/grade):.....

N° de dossier:.....

Adresse:.....

n° de téléphone: (indicatif du pays) (indicatif de zone ou urbain).....

n° de télécopieur: (indicatif du pays) (indicatif de zone ou urbain).....

Adresse électronique:.....

Date:

Cachet officiel (si disponible) et signature:.....

SECTION F: Coordonnées de l'autorité qui a validé l'EPOC

Type d'autorité qui a validé l'EPOC (cochez la case correspondante, le cas échéant):

juge, juridiction ou juge d'instruction

procureur (pour les données relatives aux abonnés *et les adresses IP aux seules fins d'identification de personnes spécifiques*)

Coordonnées de l'autorité de validation et/ou de son représentant certifiant que le contenu de l'EPOC est exact et correct:

Nom de l'autorité:.....

Nom de son représentant:.....

Fonction (titre/grade):.....

N° de dossier:.....

Adresse:

N° de téléphone: (indicatif du pays) (indicatif de zone ou urbain).....

N° de télécopieur: (indicatif du pays) (indicatif de zone ou urbain).....

Adresse électronique:.....

Date:

Cachet officiel (si disponible) et signature:.....

SECTION G Transmission des données et coordonnées

i) Autorité à qui les données doivent être transmises (cochez et complétez, le cas échéant):

autorité d'émission

autorité de validation

autre autorité compétente désignée par l'État d'émission:.....

ii) Autorité/point de contact pour toute question liée à l'exécution de l'EPOC:.....

ANNEXE II

CERTIFICAT D'INJONCTION EUROPÉENNE DE CONSERVATION (EPOC-PR) CONCERNANT LA CONSERVATION **D'INFORMATIONS** ÉLECTRONIQUES

Conformément au règlement (UE)...², le certificat d'injonction européenne de conservation (EPOC-PR) doit *être adressé directement et simultanément au fournisseur de services (ou, s'il y a lieu, à son représentant légal) et à l'autorité d'exécution en vue de l'exécution de l'EPOC-PR*. La conservation prendra fin après 60 jours, à moins que l'autorité d'émission ne confirme qu'une demande ultérieure de production a été émise. Si l'autorité d'émission confirme, dans les 60 jours, qu'une demande ultérieure de production a été émise, le destinataire doit conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande ultérieure aura été notifiée.

Les destinataires doivent prendre les mesures nécessaires pour assurer la confidentialité de l'EPOC-PR, ainsi que des données conservées ou produites.

SECTION A:

État

d'émission:

.....

Remarque: les coordonnées de l'autorité d'émission doivent être fournies à la fin du formulaire (sections D et E)

Destinataires (cochez la case appropriée et complétez):

- **le fournisseur de services ou, le cas échéant, son représentant légal:...**

- **l'autorité d'exécution:...**

SECTION B: **Informations à l'utilisateur**

Veuillez noter que (cochez le cas échéant):

le **fournisseur de services** doit s'abstenir d'informer la personne dont les données sont demandées de l'existence de l'EPOC-PR **sur la base d'une injonction judiciaire.**

Justification:...

SECTION C: **Informations** électroniques à conserver

i) le présent EPOC-PR concerne (cochez la ou les cases appropriées):

des données relatives aux abonnés :

le nom, l'adresse, la date de naissance et les coordonnées (adresse électronique, numéro de téléphone) de l'utilisateur/du titulaire de l'abonnement et d'autres informations pertinentes permettant de l'identifier

la date et l'heure du premier enregistrement, le type d'enregistrement, la copie du contrat, les moyens de vérification de l'identité utilisés au moment de l'enregistrement, des copies des documents fournis par l'abonné

le type de service, y compris l'identifiant (numéro de téléphone, numéro de carte SIM, adresse MAC) et l'appareil ou les appareils associés

des informations relatives au profil (nom d'utilisateur, photo de profil)

des données sur la validation de l'utilisation du service, comme une adresse électronique de substitution fournie par l'utilisateur/le titulaire de l'abonnement

des codes PUK

les adresses IP, aux seules fins d'identification de l'utilisateur:

- **adresse IP**

- les enregistrements/journaux des connexions IP à des fins d'identification

données concernant le trafic :

a) pour la téléphonie (mobile):

- les identifiants sortants (A) et entrants (B) (numéro de téléphone, IMSI, IMEI)
- l'heure et la durée des connexions
- les tentatives d'appel
- l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion
- le support/téléservice utilisé (par exemple UMTS, GPRS)

b) pour l'internet

- les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur, identité du message]
- l'identité de la station de base, y compris les informations géographiques (coordonnées X/Y), à l'heure de début et de fin de la connexion
- le volume de données

c) pour l'hébergement:

- les fichiers-journaux
- les tickets
- historique d'achats
- autres données relatives **au trafic** :
- l'historique de rechargement du solde prépayé

des données relatives au contenu :

- **liste de contacts**

- une boîte de messagerie (internet)
- un stockage en ligne (données générées par l'utilisateur)
- une page
- un journal/une sauvegarde de messages
- une messagerie vocale
- un contenu de serveurs
- une sauvegarde d'appareil

ii) **Informations supplémentaires nécessaires à l'exécution de l' EPOC-PR:**

adresse IP:.....
numéro de téléphone:.....
adresse électronique:.....
numéro IMEI:.....
adresse MAC:.....
personne(s) dont les données sont demandées:.....
nom du service:
autre:

iii) **Période** pour laquelle la conservation des données est demandée:

.....

iv) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC-PR est émis ainsi que disposition juridique ou code applicable:

.....
v) Autres informations utiles:
.....

SECTION D: Coordonnées de l'autorité qui a émis l'EPOC-PR

Type d'autorité qui a émis l'EPOC-PR (cochez la case appropriée):

- juge, juridiction ou juge d'instruction
- procureur
- toute autre autorité compétente désignée par l'État d'émission → veuillez compléter également la section E

Coordonnées de l'autorité d'émission et/ou de son représentant certifiant que le contenu de l'EPOC-PR est exact et correct:

Nom de l'autorité:.....

Nom de son
représentant:.....

Fonction (titre/grade):.....

N° de dossier:.....

Adresse:.....

N° de téléphone: (indicatif du pays) (indicatif de zone ou
urbain).....

N° de télécopieur: (indicatif du pays) (indicatif de zone ou
urbain).....

Adresse

électronique:.....

Date:

Cachet officiel (si disponible) et signature:.....

SECTION E: Coordonnées de l'autorité qui a validé l'EPOC-PR

Type d'autorité qui a validé l'EPOC-PR (cocher la case correspondante):

- juge, juridiction ou juge d'instruction
- procureur

Coordonnées de l'autorité de validation et/ou de son représentant certifiant que le contenu de l'EPOC-PR est exact et correct:

Nom de l'autorité:.....

Nom de son
représentant:.....

Fonction (titre/grade):.....

N° de dossier:.....

Adresse:

N° de téléphone: (indicatif du pays) (indicatif de zone ou
urbain).....

N° de télécopieur: (indicatif du pays) (indicatif de zone ou
urbain).....

Adresse

électronique:.....

Date:

Cachet officiel (si disponible) et signature:.....

SECTION F: Coordonnées

Autorité de contact pour toute question liée à l'exécution de l'EPOC-PR:

ANNEXE III

INFORMATIONS CONCERNANT L'IMPOSSIBILITÉ D'EXÉCUTER L'EPOC/EPOC-PR OU LA NON-RECONNAISSANCE DE L'EPOC

SECTION A:

Les informations suivantes concernent:

- l'injonction européenne de production (EPOC)
- l'injonction européenne de conservation (EPOC-PR)

SECTION B:

Destinataires de l'EPOC/EPOC-PR:

- le fournisseur de services ou, le cas échéant, son représentant légal:...

- l'autorité d'exécution:...

Autorité qui a émis l'EPOC/EPOC-PR:

Le cas échéant, autorité qui a validé l'EPOC/EPOC-PR:

SECTION C:

Référence du dossier du destinataire de l'EPOC/EPOC-PR:

.....

Référence du dossier de l'autorité d'émission:

.....

Le cas échéant, référence du dossier de l'autorité de validation:.....

Date de transmission de l'EPOC/EPOC-PR:

SECTION D: Raisons de l'impossibilité *d'exécuter l'EPOC/EPOC-PR*

i) L'EPOC/EPOC-PR ne peut être exécuté ou ne peut être exécuté dans le délai requis pour la ou les raisons suivantes:

- l'EPOC/EPOC-PR est incomplet
- l'EPOC/EPOC-PR contient des erreurs manifestes, **sur le fond ou sur la forme**
- l'EPOC/EPOC-PR ne contient pas suffisamment d'informations
- force majeure ou impossibilité de fait **liée à des circonstances non imputables** au destinataire ou au fournisseur de services
- l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission tel que spécifié à l'article 4 du règlement (UE)...
- l'injonction européenne de conservation n'a pas été émise ou validée par une autorité d'émission tel que spécifié à l'article 4 du règlement (UE)...
- l'injonction européenne de production n'a pas été émise pour une infraction visée à l'article 5, paragraphe 4, du règlement (UE)...
- le **fournisseur de services** ne relève pas du champ d'application du règlement (UE)...
- l'injonction européenne de production/l'injonction européenne de conservation ne concerne pas des données stockées par le fournisseur de services ou pour le compte de celui-ci au moment de **l'émission** de l'EPOC/EPOC-PR
- sur la base des seules informations contenues dans l'EPOC/EPOC-PR, il apparaît que celui-ci est manifestement **abusif ou qu'il excède l'objectif de l'injonction européenne de conservation**

□ le respect de l'injonction européenne de production *ou de l'injonction européenne de conservation* enfreindrait la législation d'un pays tiers interdisant la divulgation des données concernées.

ii) Veuillez préciser les raisons de l'impossibilité d'exécution en l'espèce, y compris, si nécessaire, en indiquant des raisons autres que celles énumérées au point i) de la présente section:

.....

SECTION D bis:

Motifs de non-reconnaissance ou de non-exécution de l'EPOC (cochez la case appropriée):

Pour tous les EPOC:

[] les conditions d'émission d'une injonction européenne de production, telles qu'elles sont établies à l'article 5 du présent règlement, ne sont pas remplies;

[] l'exécution de l'injonction européenne de production serait contraire au principe non bis in idem;

[] il existe des motifs sérieux de croire que l'exécution de l'injonction européenne de production serait incompatible avec les obligations de l'État membre au titre de l'article 6 du traité UE et de la charte;

[] il existe une immunité, un privilège ou des règles relatives à la détermination et à la restriction de la responsabilité pénale en matière de liberté de la presse et de liberté d'expression dans d'autres médias en vertu du droit de l'État d'exécution, qui rendent impossible l'exécution de l'injonction européenne de production;

Pour les EPOC concernant des données relatives au trafic et au contenu:

[] l'exécution de l'injonction européenne de production porterait préjudice à des intérêts nationaux fondamentaux en matière de sécurité, mettrait en péril la source des informations ou impliquerait l'utilisation d'informations classifiées relatives à des activités de renseignements spécifiques;

[] l'injonction européenne de production concerne une infraction pénale qui est présumée avoir été commise en dehors du territoire de l'État d'émission et, en tout ou en partie, sur le territoire de l'État d'exécution, et les faits pour lesquels l'EPOC a été émis ne constituent pas une infraction pénale selon le droit de l'État d'exécution;

[] les faits pour lesquels l'EPOC a été émis ne constituent pas une infraction au titre du droit de l'État d'exécution, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions figurant à l'annexe III bis, conformément à ce qui a été indiqué dans l'EPOC par l'autorité d'émission, si ces faits sont passibles dans l'État d'émission d'une peine ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins trois ans;

[] l'exécution de l'injonction européenne de production est limitée en vertu du droit de l'État d'exécution à une liste ou à une catégorie d'infractions ou à des infractions passibles de sanctions plus lourdes;

[] le respect de l'injonction européenne de production conduirait à enfreindre la législation d'un pays tiers interdisant la divulgation des données concernées.

SECTION E: Obligations contradictoires découlant de la législation d'un pays tiers

En cas d'obligations contradictoires découlant de la législation d'un pays tiers, veuillez fournir les informations suivantes:

- intitulé du ou des actes législatifs du pays tiers, y compris la ou les dispositions pertinentes:

.....

- texte de la ou des dispositions pertinentes:

.....

- nature de l'obligation contradictoire, y compris l'intérêt protégé par la législation du pays tiers:

droits fondamentaux des particuliers (veuillez préciser):

.....

intérêts fondamentaux du pays tiers liés à la sécurité et à la défense nationales (veuillez préciser):

.....

autres intérêts (veuillez préciser):

.....

- veuillez expliquer pourquoi la législation est applicable en l'espèce:

.....

- veuillez expliquer pourquoi vous estimez qu'il y a conflit en l'espèce:

.....

- veuillez expliquer le lien entre le fournisseur de services et le pays tiers en question:

.....

- conséquences possibles du respect de l'injonction européenne de production pour le destinataire, y compris les sanctions auxquelles il s'expose:

.....

SECTION F: Informations requises

Des informations complémentaires sont requises de la part de l'autorité d'émission afin que l'EPOC/EPOC-PR soit exécuté (complétez, le cas échéant):

.....

SECTION G Conservation des données

Les données demandées (cochez la case appropriée et complétez, le cas échéant):

seront conservées ***pour une période de cinq jours à des fins d'éclaircissement ou, si nécessaire, de rectification de la part de*** l'autorité d'émission

ne seront pas ***produites ou*** conservées étant donné que les informations fournies dans l'EPOC/EPOC-PR ne permettent pas d'identifier les données.

- ne seront pas produites étant donné que l'un des motifs de non-reconnaissance ou de non-exécution est avéré.

SECTION H Coordonnées du fournisseur de services *ou, le cas échéant,* de son représentant
légal

Nom du fournisseur de services/représentant légal:.....

Nom de la personne autorisée:.....

Cachet officiel (si disponible) et signature:.....

ANNEXE III bis

Catégories d'infractions visées à l'article 10 bis, paragraphe 2, point c):

- *participation à une organisation criminelle;*
- *terrorisme;*
- *traite d'êtres humains;*
- *exploitation sexuelle des enfants et pédopornographie;*
- *trafic de stupéfiants et de substances psychotropes;*
- *trafic d'armes, de munitions et d'explosifs;*
- *corruption;*
- *fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union européenne au sens de la convention du 26 juillet 1995 relative à la protection des intérêts financiers des Communautés européennes;*
- *blanchiment des produits du crime;*
- *faux-monnayage et contrefaçon de monnaie, y compris de l'euro;*
- *cybercriminalité;*
- *crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;*
- *aide à l'entrée et au séjour irréguliers;*
- *meurtre, coups et blessures graves;*
- *trafic d'organes et de tissus humains;*
- *enlèvement, séquestration et prise d'otage;*
- *racisme et xénophobie;*
- *vol organisé ou vol à main armée;*
- *trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;*
- *escroquerie;*
- *racket et extorsion de fonds;*
- *contrefaçon et piratage de produits;*
- *falsification de documents administratifs et trafic de faux;*
- *falsification de moyens de paiement;*
- *trafic de substances hormonales et d'autres facteurs de croissance;*
- *trafic de matières nucléaires et radioactives;*
- *trafic de véhicules volés;*
- *viol;*
- *incendie volontaire;*
- *crimes relevant de la compétence de la Cour pénale internationale;*
- *détournement d'avion/de navire;*
- *sabotage.*

PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND

Titre	Injonctions européennes de production et de conservation pour les preuves électroniques en matière pénale		
Références	COM(2018)0225 – C8-0155/2018 – 2018/0108(COD)		
Date de la présentation au PE	17.4.2018		
Commission compétente au fond Date de l'annonce en séance	LIBE 31.5.2018		
Commissions saisies pour avis Date de l'annonce en séance	IMCO 31.5.2018		
Avis non émis Date de la décision	IMCO 16.5.2018		
Rapporteurs Date de la nomination	Birgit Sippel 4.9.2019		
Examen en commission	11.11.2019	28.1.2020	7.12.2020
Date de l'adoption	7.12.2020		
Résultat du vote final	+: -: 0:	35 22 7	
Membres présents au moment du vote final	Magdalena Adamowicz, Konstantinos Arvanitis, Malik Azmani, Katarina Barley, Fernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareș Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Nicolaus Fest, Jean-Paul Garraud, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in 't Veld, Patryk Jaki, Lívia Járóka, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Nuno Melo, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Jadwiga Wiśniewska, Javier Zarzalejos		
Suppléants présents au moment du vote final	Delara Burkhardt, Andor Deli, Leopoldo López Gil, Kostas Papadakis, Anne-Sophie Pelletier, Rob Rooken, Domènec Ruiz Devesa, Hilde Vautmans, Petar Vitanov		
Date du dépôt	11.12.2020		

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION COMPÉTENTE AU FOND

35	+
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareș Bogdan, Lena Düpont, Andrzej Halicki, Jeroen Lenaers, Leopoldo López Gil, Nuno Melo, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Tomas Tobé, Javier Zarzalejos
S&D	Katarina Barley, Pietro Bartolo, Delara Burkhardt, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Łukasz Kohut, Juan Fernando López Aguilar, Javier Moreno Sánchez, Domènec Ruiz Devesa, Birgit Sippel, Petar Vitanov, Bettina Vollath,
GUE/NGL	Konstantinos Arvanitis, Fernando Barrena Arza, Cornelia Ernst, Anne-Sophie Pelletier
NI	Milan Uhrík

22	-
PPE	Andor Deli, Lívia Járóka
Renew	Malik Azmani, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Hilde Vautmans
Verts/ALE	Patrick Breyer, Saskia Bricmont, Damien Carême, Alice Kuhnke, Tineke Strik
ECR	Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Rob Rooker
NI	Kostas Papadakis, Martin Sonneborn

7	0
ID	Nicolas Bay, Nicolaus Fest, Jean-Paul Garraud, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
ECR	Assita Kanko

Légende des signes utilisés:

+ : pour

- : contre

0 : abstention