RÈGLEMENT (UE) 2023/1543 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 12 juillet 2023

relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale

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

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

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen ([1]),

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) L'Union s'est donné pour objectif de maintenir et de développer un espace de liberté, de sécurité et de justice. En vue de l'établissement progressif de cet espace, l'Union doit adopter des mesures relevant du domaine de la coopération judiciaire en matière pénale fondée sur le principe de reconnaissance mutuelle des jugements et des décisions judiciaires, principe communément considéré comme la pierre angulaire de la coopération judiciaire en matière pénale dans l'Union depuis le Conseil européen de Tampere des 15 et 16 octobre 1999.

(2) Les mesures visant à obtenir et à conserver des preuves électroniques sont de plus en plus importantes pour les enquêtes et les poursuites pénales dans l'ensemble de l'Union. Des mécanismes efficaces pour obtenir des preuves électroniques sont essentiels pour lutter contre la criminalité, et de tels mécanismes devraient être soumis à des conditions et des garanties assurant le plein respect des droits et principes fondamentaux reconnus dans l'article 6 du traité sur l'Union européenne et la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), en particulier les principes de nécessité et de proportionnalité, de procès équitable, de protection de la vie privée et des données à caractère personnel, et de confidentialité des communications.

(3) La déclaration commune des ministres de la justice et des affaires intérieures et des représentants des institutions de l'Union du 24 mars 2016 sur les attentats terroristes perpétrés à Bruxelles a souligné la nécessité, en priorité, de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement et de définir des mesures concrètes pour ce faire.

(4) Les conclusions du Conseil du 9 juin 2016 ont souligné l'importance croissante des preuves électroniques dans les procédures pénales, ainsi que l'importance de protéger le cyberespace contre les abus et les activités criminelles au profit des économies et des sociétés, et donc la nécessité pour les autorités répressives et les autorités judiciaires de disposer d'outils efficaces pour enquêter sur les actes de criminalité commis en rapport avec le cyberespace et en poursuivre les auteurs.

(5) Dans la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité au Parlement européen et au Conseil du 13 septembre 2017, intitulée «Résilience, dissuasion et défense: doter l'UE d'une cybersécurité solide», la Commission a souligné que l'efficacité des enquêtes et des poursuites relatives à la criminalité facilitée par la cybernétique constitue un moyen de dissuasion essentiel contre les cyberattaques, et que le cadre procédural actuel doit être mieux adapté à l'ère de l'internet. Les procédures actuelles peuvent être parfois dépassées par la rapidité des cyberattaques, qui crée ainsi des besoins particuliers de coopération transfrontière rapide.

(6) La résolution du Parlement européen du 3 octobre 2017 sur la lutte contre la cybercriminalité ([3]) a insisté sur la nécessité de trouver des moyens de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement, ainsi que sur l'importance que revêt une coopération étroite entre les autorités répressives, les pays tiers et les fournisseurs de services actifs sur le territoire européen, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et à la directive (UE) 2016/680 du Parlement européen et du

([1]) JO C 367 du 10.10.2018, p. 88.
([2]) Position du Parlement européen du 13 juin 2023 (non encore parue au Journal officiel) et décision du Conseil du 27 juin 2023.
([3]) JO C 346 du 27.9.2018, p. 29.
([4]) 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).

Conseil ([5]) ainsi qu'aux accords actuels en matière d'entraide judiciaire. Cette résolution du Parlement européen a souligné également que le cadre juridique actuellement fragmenté peut poser des difficultés aux fournisseurs de services qui s'efforcent de répondre favorablement aux demandes des services répressifs, et a invité la Commission à proposer un cadre juridique de l'Union pour les preuves électroniques offrant des garanties suffisantes concernant les droits et les libertés de toutes les parties concernées, tout en saluant les travaux actuels de la Commission portant sur la création d'une plateforme de coopération munie d'un canal de communication sécurisé permettant l'échange de décisions d'enquête européennes par voie numérique, en ce qui concerne les preuves électroniques et les réponses entre les autorités judiciaires de l'Union.

(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 où le service en question est proposé. Par conséquent, les preuves électroniques pertinentes sont souvent stockées en dehors de l'État menant l'enquête ou par un fournisseur de services établi en dehors de cet État, ce qui rend difficile l'obtention de preuves électroniques dans les procédures pénales.

(8) En raison de la manière dont les services basés sur un réseau sont fournis, 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 s'est multiplié en raison de l'utilisation croissante des services basés sur un réseau. La directive 2014/41/UE du Parlement européen et du Conseil ([6]) prévoit la possibilité d'émettre une décision d'enquête européenne en vue de l'obtention de preuves dans un autre État membre. En outre, la convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne ([7]) (ci-après dénommée «convention relative à l'entraide judiciaire en matière pénale») prévoit elle aussi la possibilité de demander des preuves à un autre État membre. Cependant, les procédures et délais prévus dans la directive 2014/41/UE établissant la décision d'enquête européenne et dans la convention relative à l'entraide judiciaire en matière pénale pourraient ne pas convenir pour les preuves électroniques, qui sont plus éphémères et qui pourraient être plus rapidement et facilement supprimées. L'obtention de preuves électroniques par les canaux de coopération judiciaire prend souvent beaucoup de temps, ce qui aboutit à des situations où les pistes auxquelles ces preuves auraient pu mener risquent de disparaître. 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 autres que les données relatives au contenu, conformément à leur droit national applicable. En conséquence, les États membres s'appuient de plus en plus sur des canaux impliquant la coopération volontaire directe des fournisseurs de services, lorsque ces canaux existent, et utilisent des outils nationaux différents et appliquent des conditions et procédures nationales différentes. Pour les données relatives au contenu, certains États membres ont pris des mesures unilatérales, tandis que d'autres continuent de s'appuyer sur la coopération judiciaire.

(9) La fragmentation du cadre juridique entraîne des difficultés pour les autorités répressives et les autorités judiciaires ainsi que pour les fournisseurs de services qui cherchent à se conformer aux demandes légales de preuves électroniques, car ils se heurtent de plus en plus à l'incertitude juridique et, potentiellement, à des conflits de lois. Par conséquent, il est nécessaire de prévoir des règles spécifiques de coopération judiciaire transfrontière pour la conservation et la production de preuves électroniques, qui soient adaptées à la nature spécifique des preuves électroniques. Ces règles devraient comprendre l'obligation, pour les fournisseurs de services relevant du champ d'application du présent règlement, de répondre directement aux demandes émanant des autorités dans un autre État membre. Le présent règlement complètera dès lors le droit de l'Union en vigueur et précisera les règles applicables aux autorités répressives et aux autorités judiciaires, ainsi qu'aux fournisseurs de services, en matière de preuves électroniques, tout en garantissant le plein respect des droits fondamentaux.

(10) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus par l'article 6 du traité sur l'Union européenne et la Charte, par le droit international et par 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 par les Constitutions des États membres, dans leur champ d'application respectif. Ces droits et principes comprennent, en particulier, le droit à la liberté et à la sûreté, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité, ainsi que le droit de ne pas être jugé ou puni pénalement deux fois pour une même infraction.

([5]) 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).

([6]) 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).

([7]) Convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (JO C 197 du 12.7.2000, p. 3).

(11) Rien dans le présent règlement ne peut être interprété comme interdisant à une autorité chargée de la mise en œuvre de refuser 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 son origine raciale ou ethnique, 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'il pourrait être porté atteinte à la situation de cette personne pour l'une de ces raisons.

(12) Le mécanisme de l'injonction européenne de production et de l'injonction européenne de conservation de preuves électroniques dans les procédures pénales fonctionne sur la base du principe de confiance mutuelle entre les États membres et sur la base d'une présomption de respect par les États membres du droit de l'Union, de l'état de droit et, notamment, des droits fondamentaux, qui constituent des éléments essentiels de l'espace de liberté, de sécurité et de justice de l'Union. Un tel mécanisme permet aux autorités nationales compétentes d'adresser ces injonctions directement aux fournisseurs de services.

(13) 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, 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.

(14) Lors de la mise en œuvre du présent règlement, les États membres devraient veiller à ce que les données à caractère personnel soient protégées et traitées conformément au règlement (UE) 2016/679 et à la directive (UE) 2016/680 ainsi qu'à la directive 2002/58/CE du Parlement européen et du Conseil [8], y compris en cas de réutilisation, de transmission ou de transfert ultérieur des données obtenues.

(15) Les données à caractère personnel obtenues dans le cadre du présent règlement ne devraient être traitées que lorsque cela est nécessaire et d'une manière qui soit proportionnée aux objectifs de prévention, de détection et de poursuite de la criminalité, et d'enquêtes en la matière, ou d'exécution de sanctions pénales, et à l'exercice des droits de la défense. Les États membres devraient veiller en particulier à ce que des politiques et des mesures appropriées en matière 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 veiller à ce que les mêmes garanties s'appliquent 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 auxquelles il est possible d'avoir accès par des processus d'authentification.

(16) Les droits procéduraux dans les procédures pénales énoncés dans les directives 2010/64/UE [9], 2012/13/UE [10], 2013/48/UE [11], (UE) 2016/343 [12], (UE) 2016/800 [13] et (UE) 2016/1919 [14] du Parlement européen et du Conseil devraient s'appliquer, dans les limites du champ d'application desdites directives, aux procédures pénales relevant du champ d'application du présent règlement en ce qui concerne les États membres liés par les directives en question. Les garanties procédurales prévues par la Charte devraient s'appliquer également.

(17) Afin de garantir le plein respect des droits fondamentaux, la valeur probante des preuves obtenues en application du présent règlement devrait être évaluée au cours du procès par l'autorité judiciaire compétente, conformément au droit national et dans le respect, en particulier, du droit à un procès équitable et des droits de la défense.

[8] 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 vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

[9] 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).

[10] 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).

[11] 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).

[12] 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).

[13] 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).

[14] 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).

(18) Le présent règlement fixe les règles selon lesquelles une autorité judiciaire compétente dans l'Union peut, dans le cadre d'une procédure pénale, y compris d'une enquête pénale, ou aux fins de l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté prononcées à l'issue d'une procédure pénale conformément au présent règlement, ordonner à un fournisseur de services proposant des services dans l'Union de produire ou de conserver des preuves électroniques au moyen d'une injonction européenne de production ou d'une injonction européenne de conservation. Le présent règlement devrait s'appliquer dans tous les cas transfrontières où le fournisseur de services a son établissement désigné ou son représentant légal dans un autre État membre. Le présent règlement est sans préjudice des pouvoirs des autorités nationales de s'adresser aux fournisseurs de services établis ou représentés sur leur territoire afin qu'ils se conforment à des mesures nationales similaires.

(19) Le présent règlement devrait réglementer uniquement l'obtention des données stockées par un fournisseur de services au moment de la réception d'une injonction européenne de production ou d'une injonction européenne de conservation. Il ne devrait pas prévoir d'obligation générale de conservation des données applicable aux fournisseurs de services et ne devrait pas avoir pour effet d'entraîner une conservation générale et indifférenciée des données. Le présent règlement ne devrait pas non plus autoriser l'interception de données ou l'obtention de données qui sont stockées après la réception d'une injonction européenne de production ou d'une injonction européenne de conservation.

(20) L'application du présent règlement ne devrait pas avoir de répercussions sur le recours au chiffrement par les fournisseurs de services ou leurs utilisateurs. Les données demandées au moyen d'une injonction européenne de production ou d'une injonction européenne de conservation devraient être fournies ou conservées, que ces données soient chiffrées ou non. Toutefois, le présent règlement ne devrait pas imposer une obligation pour les fournisseurs de services de déchiffrer des données.

(21) Dans de nombreux cas, les données ne sont plus stockées ou traitées d'une autre manière sur le dispositif d'un utilisateur, mais rendues disponibles sur une infrastructure en nuage permettant d'y accéder à partir de n'importe quel endroit. Pour opérer ces services, les fournisseurs de services n'ont pas besoin d'être établis ou d'avoir des serveurs sur un territoire spécifique. Ainsi, l'application du présent règlement ne devrait pas dépendre de la localisation réelle de l'établissement du fournisseur de services ou de l'installation de traitement ou de stockage des données.

(22) Le présent règlement est sans préjudice des pouvoirs d'enquête des autorités dans les procédures civiles ou administratives, notamment lorsque ces procédures peuvent entraîner des sanctions.

(23) Les procédures en matière d'entraide judiciaire pouvant être considérées comme des procédures pénales selon le droit national applicable dans les États membres, il y a lieu de préciser qu'une injonction européenne de production ou une injonction européenne de conservation ne devrait pas être émise pour fournir une entraide judiciaire à un autre État membre ou à un pays tiers. Dans ce cas, la demande d'entraide judiciaire devrait être adressée à l'État membre ou au pays tiers qui peut fournir une entraide judiciaire en vertu de son droit national.

(24) Dans le cadre de procédures pénales, l'injonction européenne de production et l'injonction européenne de conservation ne devraient être émises que pour des procédures pénales spécifiques concernant une infraction pénale spécifique qui a déjà été commise, après une évaluation dans chaque cas de la nécessité et de la proportionnalité, en tenant compte des droits du suspect ou de la personne poursuivie.

(25) Le présent règlement devrait s'appliquer également aux procédures engagées par une autorité d'émission en vue de localiser une personne condamnée qui s'est soustraite à la justice, afin d'exécuter une peine ou une mesure de sûreté privatives de liberté prononcées à l'issue d'une procédure pénale. Cependant, au cas où la peine ou mesure de sûreté privatives de liberté ont été prononcées par une décision de justice rendue par défaut, il ne devrait pas être possible d'émettre une injonction européenne de production ou une injonction européenne de conservation, étant donné que le droit national en matière de décisions de justice rendues par défaut varie considérablement d'un État membre à l'autre au sein de l'Union.

(26) Le présent règlement s'applique aux fournisseurs de services qui proposent des services dans l'Union, et il ne devrait être possible d'émettre les injonctions prévues dans le présent règlement que pour les données relatives aux services proposés dans l'Union. Les services proposés exclusivement en dehors de l'Union ne devraient pas relever du champ d'application du présent règlement, même si le fournisseur de services est établi dans l'Union. Par conséquent, le présent règlement ne devrait permettre aucun accès à des données autres que celles relatives aux services proposés à l'utilisateur dans l'Union par ces fournisseurs de services.

(27) Les fournisseurs de services présentant le plus d'intérêt pour l'obtention de preuves dans le cadre des procédures pénales sont les fournisseurs de services de communications électroniques et certains fournisseurs de services de la société de l'information qui facilitent les interactions entre les utilisateurs. Dès lors, ces deux groupes devraient être couverts par le présent règlement. Les services de communications électroniques sont définis dans la directive (UE) 2018/1972 du Parlement européen et du Conseil ([15]) et comprennent les services de communications

([15]) 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).

interpersonnelles tels que la voix par le protocole de l'internet (IP), la messagerie instantanée et les services de courrier électronique. Le présent règlement devrait aussi s'appliquer aux fournisseurs de services de la société de l'information, au sens de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([16]), qui ne sont pas considérés comme des fournisseurs de services de communications électroniques, mais qui offrent à leurs utilisateurs la possibilité de communiquer les uns avec les autres ou qui proposent à leurs utilisateurs des services qui peuvent être utilisés pour stocker ou traiter d'une autre manière des données pour leur compte. Cette approche serait conforme aux termes utilisés dans la convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185), signée à Budapest le 23 novembre 2001 (ci-après dénommée «convention de Budapest»). Le traitement des données devrait être compris au sens technique de création ou de manipulation de données, c'est-à-dire des opérations techniques destinées à produire ou modifier des données en faisant appel à la puissance de traitement des ordinateurs. Les catégories de fournisseurs de services relevant du champ d'application du présent règlement devraient comprendre, par exemple, les places de marché en ligne offrant aux consommateurs et aux entreprises la possibilité de communiquer les uns avec les autres, et les autres services d'hébergement, notamment lorsque le service est fourni par l'intermédiaire de l'informatique en nuage, ainsi que les plateformes de jeux en ligne et les plateformes de jeux d'argent et de hasard en ligne. Lorsqu'un fournisseur de services de la société de l'information n'offre pas à ses utilisateurs la possibilité de communiquer les uns avec les autres, mais uniquement la possibilité de communiquer avec le fournisseur de services, ou n'offre pas la possibilité de stocker ou de traiter d'une autre manière des données ou lorsque le stockage de données ne constitue pas une composante déterminante, c'est-à-dire une partie essentielle, du service fourni aux utilisateurs, tels que les services juridiques ou les services d'architecture, d'ingénierie et de comptabilité fournis à distance en ligne, ce fournisseur ne devrait pas entrer dans le champ de la définition de «fournisseur de services» prévue par le présent règlement, et ce même si les services qu'il fournit sont des services de la société de l'information au sens de la directive (UE) 2015/1535.

(28) Les fournisseurs de services d'infrastructure internet liés à l'attribution de noms et de numéros, tels que les registres et les bureaux d'enregistrement de noms de domaine et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, ou les registres internet régionaux pour les adresses de protocole de l'internet (IP), présentent un intérêt particulier lorsqu'il s'agit d'identifier des acteurs cachés derrière des sites internet malveillants ou compromis. Ils détiennent des données qui pourraient permettre l'identification d'une personne ou d'une entité cachée derrière un site internet utilisé dans une activité criminelle, ou de la victime d'une activité criminelle.

(29) Pour déterminer si un fournisseur de services fournit des services dans l'Union, il est nécessaire d'évaluer si le fournisseur de services permet à des personnes physiques ou morales dans un ou plusieurs États membres d'utiliser ses services. Toutefois, la seule accessibilité d'une interface en ligne dans l'Union, comme par exemple l'accessibilité d'un site internet, d'une adresse électronique ou d'autres coordonnées de contact d'un fournisseur de services ou d'un intermédiaire, prise isolément, devrait être considérée comme insuffisante pour déterminer si un fournisseur de services propose des services dans l'Union au sens du présent règlement.

(30) Un lien substantiel avec l'Union devrait également être pertinent pour déterminer si un fournisseur de services propose des services dans l'Union. Un tel lien substantiel avec l'Union devrait être considéré exister lorsque le fournisseur de services dispose d'un établissement dans l'Union. En l'absence d'un tel établissement, le critère de lien substantiel devrait être basé sur des critères factuels spécifiques, tels que l'existence d'un nombre significatif d'utilisateurs dans un ou plusieurs États membres, ou le ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités sur un ou plusieurs États membres devrait être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet État membre, ou la possibilité de commander des biens ou des services. Le ciblage des activités sur un État membre pourrait également être constaté sur la base de la disponibilité d'une application («appli») dans la boutique d'applications nationale correspondante, de la diffusion de publicité locale ou de publicité dans la langue généralement utilisée dans cet État membre ou de la gestion des relations avec la clientèle, comme, par exemple, la fourniture d'un service à la clientèle dans la langue généralement utilisée dans cet État membre. Un lien substantiel devrait également être considéré exister lorsqu'un fournisseur de services dirige ses activités vers un ou plusieurs États membres comme le mentionne le règlement (UE) n° 1215/2012 du Parlement européen et du Conseil ([17]). En revanche, fournir un service dans le simple but de se conformer à l'interdiction de discrimination prévue par le règlement (UE) 2018/302 du Parlement européen et du Conseil ([18]) ne devrait pas, en l'absence d'autres motifs, être considéré comme diriger ou cibler des activités vers un territoire donné au sein de l'Union. Les mêmes considérations devraient s'appliquer pour déterminer si un fournisseur de services propose des services dans un État membre donné.

([16]) 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).

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

([18]) Règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n° 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE (JO L 60 I du 2.3.2018, p. 1).

(31) Il convient que le présent règlement couvre les catégories de données que sont les données relatives aux abonnés, les données relatives au trafic et les données relatives au contenu. Cette catégorisation est conforme au droit de nombreux États membres et au droit de l'Union, notamment à la directive 2002/58/CE et à la jurisprudence de la Cour de justice, ainsi qu'au droit international, notamment à la convention de Budapest.

(32) Les adresses IP ainsi que les numéros d'accès et les informations connexes peuvent constituer un point de départ essentiel pour les enquêtes pénales dans lesquelles l'identité d'un suspect n'est pas connue. Ces données sont généralement consignées dans un relevé d'événements, connu également sous le nom de «journal de serveur», qui indique le début et la fin d'une session d'accès d'un utilisateur à un service. Il s'agit souvent d'une adresse IP individuelle, qu'elle soit statique ou dynamique, ou d'un autre identifiant qui distingue l'interface réseau utilisée lors de la session d'accès. Des informations connexes portant sur le début et la fin d'une session d'accès d'un utilisateur à un service, telles que les ports de provenance et l'horodatage, sont nécessaires, étant donné que les adresses IP sont souvent partagées entre plusieurs utilisateurs, par exemple lorsqu'une traduction d'adresses de réseau de classe transporteur (CGN) ou des équivalents techniques sont en place. Toutefois, conformément à l'acquis de l'Union, les adresses IP doivent être considérées comme des données à caractère personnel et bénéficier de la protection complète prévue par l'acquis de l'Union en matière de protection des données. En outre, dans certains cas, les adresses IP peuvent être considérées comme des données relatives au trafic. Par ailleurs, les numéros d'accès et les informations connexes sont eux aussi considérés comme des données relatives au trafic dans certains États membres. Toutefois, aux fins d'une enquête pénale spécifique, les autorités répressives peuvent avoir besoin de demander une adresse IP, des numéros d'accès et des informations connexes d'un utilisateur à la seule fin d'identifier ce dernier, avant de pouvoir demander au fournisseur de services les données relatives aux abonnés liées à cet identifiant. Dans ce cas, il convient d'appliquer le même régime que pour les données relatives aux abonnés, tel qu'il est défini dans le présent règlement.

(33) Lorsque des adresses IP, des numéros d'accès et des informations connexes ne sont pas demandés à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique, ils sont en général demandés pour obtenir des informations qui portent davantage atteinte à la vie privée, telles que les contacts ou la localisation de l'utilisateur. À ce titre, ils pourraient être utilisés pour dessiner un profil complet de la personne concernée, mais en même temps ils peuvent être traités et analysés plus facilement que les données relatives au contenu, étant donné qu'ils sont présentés dans un format standardisé et structuré. Il est dès lors indispensable que, dans ce cas, les adresses IP, les numéros d'accès et les informations connexes qui ne sont pas demandés à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique soient traités comme des données relatives au trafic et que la demande de telles données soit soumise au même régime que la demande de données relatives au contenu, tel qu'il est défini dans le présent règlement.

(34) 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. Cependant, l'intensité de l'incidence sur les droits fondamentaux varie d'une catégorie à l'autre, en particulier entre les données relatives aux abonnés et les données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, d'une part, et les données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, et les données relatives au contenu d'autre part. Alors que les données relatives aux abonnés ainsi que les adresses IP, les numéros d'accès et les informations connexes, lorsque ces données sont demandées à la seule fin d'identifier l'utilisateur, pourraient être utiles pour obtenir de premiers indices dans une enquête sur l'identité d'un suspect, les données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, et les données relatives au contenu sont souvent plus pertinentes en tant qu'éléments ayant valeur probante. Il est donc essentiel que toutes ces catégories de données soient couvertes par le présent règlement. Compte tenu des degrés variables d'interférence avec les droits fondamentaux, des garanties et des conditions appropriées devraient être imposées pour obtenir de telles données.

(35) Les situations dans lesquelles il existe une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne devraient être traitées comme des cas d'urgence et supposer un raccourcissement des délais pour le fournisseur de services et l'autorité chargée de la mise en œuvre. Lorsque l'arrêt ou la destruction d'une infrastructure critique au sens de la directive 2008/114/CE du Conseil ([19]) entraînerait une telle menace, y compris par le biais d'une atteinte grave à l'approvisionnement de base de la population ou à l'exercice des fonctions essentielles de l'État, une telle situation devrait elle aussi être traitée comme un cas d'urgence, conformément au droit de l'Union.

(36) Lorsqu'une injonction européenne de production ou une injonction européenne de conservation est émise, une autorité judiciaire devrait toujours être impliquée soit dans le processus d'émission soit dans le processus de validation de l'injonction. Compte tenu du caractère plus sensible des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, et des données relatives au contenu, l'émission ou la validation d'une injonction européenne de production visant à obtenir ces catégories de données nécessite le réexamen par un juge. Les données relatives aux abonnés et les

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

données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, étant moins sensibles, une injonction européenne de production visant à obtenir de telles données peut également être émise ou validée par un procureur compétent. Conformément au droit à un procès équitable, tel qu'il est consacré par la Charte et par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, les procureurs doivent exercer leurs compétences de manière objective et prendre leur décision concernant l'émission ou la validation d'une injonction européenne de production ou d'une injonction européenne de conservation en se fondant exclusivement sur les éléments factuels du dossier et en tenant compte de toutes les preuves à charge et à décharge.

(37) Afin de garantir la protection intégrale des droits fondamentaux, toute validation d'une injonction européenne de production ou d'une injonction européenne de conservation par des autorités judiciaires devrait en principe être obtenue avant l'émission de l'injonction en question. Il ne devrait être possible de déroger à ce principe que dans des cas d'urgence dont l'existence est établie de manière valable et en liaison avec une demande de production de données relatives aux abonnés ou de données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou avec une demande de conservation de données, lorsqu'il n'est pas possible d'obtenir à temps la validation préalable par l'autorité judiciaire, en particulier parce qu'il n'est pas possible de joindre l'autorité de validation pour obtenir cette validation et que la menace est à ce point imminente qu'une mesure immédiate doit être prise. Cependant, de telles exceptions ne devraient être possibles que lorsque l'autorité d'émission de l'injonction en question est en mesure, dans le cadre d'une procédure nationale similaire, d'émettre une injonction sans validation préalable en vertu du droit national.

(38) Une injonction européenne de production ne peut être émise que si elle s'avère nécessaire, proportionnée, adéquate et applicable au cas d'espèce. L'autorité d'émission devrait tenir compte des droits du suspect ou de la personne poursuivie dans les procédures liées à une infraction pénale et devrait émettre une injonction européenne de production uniquement lorsqu'une telle injonction aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire. Pour évaluer s'il y a lieu d'émettre une injonction européenne de production, l'autorité d'émission devrait examiner si une telle injonction est limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime d'obtenir les données pertinentes et nécessaires pour servir de preuve dans le cas d'espèce.

(39) Dans les cas où une injonction européenne de production est émise en vue d'obtenir différentes catégories de données, l'autorité d'émission devrait veiller à ce que les conditions et procédures, telle que la notification à l'autorité chargée de la mise en œuvre, soient respectées pour chacune des catégories de données concernées.

(40) Compte tenu du caractère plus sensible des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, et des données relatives au contenu, il convient d'opérer une distinction en ce qui concerne le champ d'application matériel du présent règlement. Il devrait être possible d'émettre une injonction européenne de production visant à obtenir des données relatives aux abonnés ou des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, pour toute infraction pénale; en revanche, l'émission d'une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou à obtenir des données relatives au contenu devrait être soumise à des exigences plus strictes, pour refléter la nature plus sensible de ces données. Le présent règlement devrait prévoir un seuil pour ce qui est de son champ d'application, afin de permettre une approche proportionnée, en combinaison avec un certain nombre d'autres conditions et garanties ex ante et ex post pour assurer le respect de la proportionnalité et des droits des personnes concernées. En même temps, un tel seuil ne devrait pas limiter l'efficacité du présent règlement ni son utilisation par les praticiens. Autoriser l'émission d'injonctions européennes de production dans des procédures pénales uniquement pour des infractions assorties d'une peine privative de liberté d'une durée maximale d'au moins trois ans limitera le champ d'application du présent règlement à des infractions plus graves, sans affecter de façon excessive ses possibilités d'utilisation par les praticiens. Cette limitation exclurait du champ d'application du présent règlement un nombre significatif d'infractions considérées comme moins graves par les États membres, qui donnent lieu à une peine maximale inférieure. Cette limitation aura également l'avantage d'être plus facile à appliquer dans la pratique.

(41) Il existe des infractions spécifiques pour lesquelles les preuves sont généralement disponibles exclusivement sous une forme numérique, qui est une forme par nature particulièrement éphémère. C'est le cas des infractions relevant de la cybercriminalité, même celles qui pourraient ne pas être considérées comme graves en tant que telles mais qui pourraient causer des préjudices étendus ou considérables, en particulier les infractions pour lesquelles le préjudice individuel est faible mais qui sont nombreuses et cause un préjudice global élevé. Dans la plupart des cas dans lesquels 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, en grande partie, à l'impunité. Cela justifie l'application du présent règlement à ce type d'infractions également lorsque ces infractions sont assorties d'une peine privative de liberté d'une durée maximale de moins de trois ans. Les infractions supplémentaires liées au terrorisme au sens de la directive (UE) 2017/541 du Parlement européen et du Conseil ([20]) ainsi que les infractions

([20]) 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).

relatives aux abus sexuels et à l'exploitation sexuelle des enfants au sens de la directive 2011/93/UE du Parlement européen et du Conseil ([21]) ne devraient pas requérir le seuil minimal relatif à une peine privative de liberté d'une durée maximale de trois ans.

(42) En principe, une injonction européenne de production devrait être adressée au fournisseur de services agissant en qualité de responsable du traitement. Toutefois, dans certains cas, il peut s'avérer particulièrement difficile de déterminer si un fournisseur de services agit en qualité de responsable du traitement ou en qualité de sous-traitant, notamment lorsque plusieurs fournisseurs de services sont impliqués dans le traitement des données où lorsque des fournisseurs de services traitent des données pour le compte d'une personne physique. Faire la différence entre le rôle de responsable du traitement et celui de sous-traitant pour un ensemble de données précis non seulement nécessite une connaissance spécialisée du contexte juridique, mais pourrait également nécessiter d'interpréter des cadres contractuels souvent très complexes prévoyant, dans un cas de figure précis, l'attribution, pour un ensemble de données précis, de différentes tâches et de différents rôles à plusieurs fournisseurs de services. Lorsque des fournisseurs de services traitent des données pour le compte d'une personne physique, il peut s'avérer difficile, dans certains cas, de déterminer qui est le responsable du traitement, même lorsqu'un seul fournisseur de services est concerné. Lorsque les données en question sont stockées ou traitées d'une autre manière par un fournisseur de services et que l'identité du responsable du traitement des données demeure ambigüe malgré des efforts raisonnables de la part de l'autorité d'émission, il devrait dès lors être possible d'adresser une injonction européenne de production directement à ce fournisseur de services. En outre, dans certains cas, s'adresser au responsable du traitement pourrait nuire à l'enquête dans le cas concerné, par exemple parce que le responsable du traitement est un suspect, une personne poursuivie ou une personne condamnée, ou parce qu'il existe des éléments indiquant que le responsable du traitement pourrait être en train d'agir dans l'intérêt de la personne faisant l'objet de l'enquête. Dans ce cas également, il devrait être possible d'adresser l'injonction européenne de production directement au fournisseur de services qui traite les données pour le compte du responsable du traitement. Cette possibilité ne devrait pas affecter le droit de l'autorité d'émission d'ordonner au fournisseur de services de conserver les données.

(43) Conformément au règlement (UE) 2016/679, le sous-traitant qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement devrait informer celui-ci de la production des données, sauf si l'autorité d'émission a demandé au fournisseur de services de s'abstenir d'informer le responsable du traitement, aussi longtemps que cela est nécessaire et proportionné, afin de ne pas entraver la procédure pénale concernée. Dans ce cas, l'autorité d'émission devrait indiquer dans le dossier les raisons du retard pris pour informer le responsable du traitement et une brève justification devrait également être ajoutée au certificat d'accompagnement transmis au destinataire.

(44) Lorsque les données sont stockées ou traitées d'une autre manière dans le cadre d'une infrastructure fournie par un fournisseur de services à une autorité publique, il ne devrait être possible d'émettre une injonction européenne de production ou une injonction européenne de conservation que si l'autorité publique pour laquelle les données sont stockées ou traitées d'une autre manière est située dans l'État d'émission.

(45) Lorsque des données protégées par le secret professionnel en vertu du droit de l'État d'émission sont stockées ou traitées d'une autre manière par un fournisseur de services dans le cadre d'une infrastructure fournie à des professionnels soumis au secret professionnel («professionnel soumis au secret professionnel»), dans le cadre de leur activité professionnelle, il ne devrait être possible d'émettre une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou visant à obtenir des données relatives au contenu lorsque le professionnel soumis au secret professionnel réside dans l'État d'émission, que lorsque le fait de s'adresser à ce professionnel soumis au secret professionnel pourrait nuire à l'enquête, ou lorsque le secret professionnel a été levé conformément au droit applicable.

(46) Le principe ne bis in idem est un principe de droit fondamental dans l'Union, consacré par la Charte et développé par la jurisprudence de la Cour de justice de l'Union européenne. Si l'autorité d'émission a des raisons de croire qu'une procédure pénale parallèle pourrait être en cours dans un autre État membre, elle devrait consulter les autorités de cet État membre conformément à la décision-cadre 2009/948/JAI du Conseil ([22]). En tout état de cause, une injonction européenne de production ou une injonction européenne de conservation ne peut pas être émise lorsque l'autorité d'émission a des raisons de croire que ce serait contraire au principe ne bis in idem.

(47) Les immunités et les privilèges, qui peuvent concerner des catégories de personnes, comme les diplomates, ou des relations spécifiquement protégées, comme le secret professionnel dans la relation entre l'avocat et son client ou le droit des journalistes de ne pas révéler leurs sources d'information, sont mentionnés dans d'autres instruments de reconnaissance mutuelle tels que la directive 2014/41/UE établissant la décision d'enquête européenne. La portée et l'incidence des immunités et des privilèges diffèrent selon le droit national applicable qui devrait être pris en considération au moment de l'émission d'une injonction européenne de production ou d'une injonction

([21]) 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).

([22]) 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).

européenne de conservation, étant donné que l'autorité d'émission ne devrait pouvoir émettre l'injonction que lorsqu'une telle injonction aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire. Il n'y a pas de définition commune de ce qui constitue une immunité ou un privilège dans le droit de l'Union. La définition précise de ces termes relève donc du droit national, et la définition peut englober la protection applicable notamment aux professions médicales et juridiques, y compris lorsque des plateformes spécialisées sont utilisées par ces professions. La définition précise des immunités et des privilèges peut également comprendre des règles relatives à la détermination et à la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias.

(48) Lorsque l'autorité d'émission cherche à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou à obtenir des données relatives au contenu, au moyen d'une injonction européenne de production, et qu'elle a des motifs raisonnables de croire que les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre ou que lesdites données sont soumises, dans cet État, à des règles relatives à la détermination et à la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, l'autorité d'émission devrait pouvoir demander des éclaircissements avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État chargé de la mise en œuvre, soit directement, soit par l'intermédiaire d'Eurojust ou du réseau judiciaire européen.

(49) Il devrait être possible d'émettre une injonction européenne de conservation pour n'importe quelle infraction pénale. L'autorité d'émission devrait tenir compte des droits du suspect ou de la personne poursuivie dans les procédures liées à une infraction pénale et devrait émettre une injonction européenne de conservation uniquement lorsqu'une telle injonction aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire et lorsqu'elle est nécessaire, proportionnée, adéquate et pertinente pour le cas d'espèce. Pour évaluer s'il y a lieu d'émettre une injonction européenne de conservation, l'autorité d'émission devrait examiner si une telle injonction est limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime d'empêcher le retrait, la suppression ou la modification de données qui sont pertinentes et nécessaires pour servir de preuves dans un cas d'espèce dans des situations où la production de ces données pourrait prendre plus de temps.

(50) Les injonctions européennes de production et les injonctions européennes de conservation devraient être adressées directement à l'établissement désigné ou au représentant légal, désigné par le fournisseur de services en vertu de la directive (UE) 2023/1544 du Parlement européen et du Conseil ([23]). Exceptionnellement, dans les cas d'urgence tels qu'ils sont définis par le présent règlement, lorsque l'établissement désigné ou le représentant légal d'un fournisseur de services ne réagit pas au certificat d'accompagnement de l'injonction européenne de production (EPOC) ou au certificat d'accompagnement de l'injonction européenne de conservation (EPOC-PR) dans les délais ou n'a pas été désigné dans les délais fixés par la directive (UE) 2023/1544, il devrait être possible d'adresser l'EPOC ou l'EPOC-PR à tout autre établissement ou représentant légal du fournisseur de services dans l'Union tout en poursuivant la mise en œuvre de l'injonction initiale conformément au présent règlement, ou pour remplacer la poursuite de cette mise en œuvre. Compte tenu de ces différents scénarios possibles, le terme général de «destinataire» est utilisé dans les dispositions du présent règlement.

(51) Compte tenu du caractère plus sensible d'une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou visant à obtenir des données relatives au contenu, il y a lieu de prévoir un mécanisme de notification applicable aux injonctions européennes de production visant à obtenir ces catégories de données. Ce mécanisme de notification devrait impliquer une autorité chargée de la mise en œuvre et consister en la transmission de l'EPOC à cette autorité en même temps que l'EPOC est transmis au destinataire. Cependant, lorsqu'une injonction européenne de production est émise en vue d'obtenir des preuves électroniques dans des procédures pénales ayant des liens forts et substantiels avec l'État d'émission, il n'y a pas lieu d'exiger une notification à l'autorité chargée de la mise en œuvre. De tels liens sont réputés exister lorsque, au moment de l'émission de l'injonction européenne de production, l'autorité d'émission a des motifs raisonnables de croire que l'infraction a été commise, est en train d'être commise ou est susceptible d'être commise dans l'État d'émission et lorsque la personne dont les données sont demandées réside dans l'État d'émission.

(52) Aux fins du présent règlement, il y a lieu de considérer qu'une infraction a été commise, est en train d'être commise ou est susceptible d'être commise dans l'État d'émission si elle est considérée comme telle conformément au droit national de l'État d'émission. Dans certains cas, en particulier dans le domaine de la cybercriminalité, certains éléments factuels, tels que le lieu de résidence de la victime, constituent, en règle générale, des indications importantes qu'il y a lieu de prendre en compte lorsqu'il s'agit de déterminer le lieu de commission de l'infraction. Par exemple, les crimes commis au moyen d'un rançongiciel peuvent souvent être considérés comme ayant été commis sur le lieu de résidence de la victime d'un tel crime, même lorsque la localisation exacte de l'endroit d'où le rançongiciel a été lancé est incertaine. Toute détermination du lieu de commission d'une infraction devrait être sans préjudice des règles de détermination de la compétence pour connaître de l'infraction en question définies dans le droit national applicable.

([23]) Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (voir page 181 du présent Journal officiel).

(53) Il incombe à l'autorité d'émission d'évaluer, au moment où elle émet une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou visant à obtenir des données relatives au contenu, sur la base des éléments dont elle dispose, s'il existe des motifs raisonnables de croire que la personne dont les données sont demandées réside dans l'État d'émission. À cet égard, plusieurs circonstances factuelles qui pourraient indiquer que la personne concernée a établi le centre habituel de ses intérêts dans un État membre donné ou a l'intention de le faire peuvent s'avérer pertinentes. Il découle de la nécessité d'une application uniforme du droit de l'Union, ainsi que du principe d'égalité, que la notion de «résidence», dans ce contexte précis, devrait être interprétée de manière uniforme dans l'ensemble de l'Union. L'on peut notamment considérer comme un motif raisonnable de croire qu'une personne réside dans un État d'émission le fait qu'une personne soit enregistrée comme résidente dans un État d'émission, comme attesté par la détention d'une pièce d'identité ou d'un permis de séjour ou par le fait d'être inscrit dans un registre officiel des résidents. En l'absence d'enregistrement dans l'État d'émission, la résidence pourrait être déduite du fait qu'une personne a manifesté l'intention de s'installer dans cet État membre ou a établi, à l'issue d'une période stable de présence dans cet État membre, certains liens avec cet État dont la force est similaire à celle des liens résultant de l'établissement d'une résidence formelle dans cet État membre. Afin de déterminer si, dans un cas précis, il existe suffisamment de liens entre la personne concernée et l'État d'émission pour qu'il existe des motifs raisonnables de croire que la personne concernée réside dans cet État, il convient de tenir compte de plusieurs facteurs objectifs caractérisant la situation de cette personne, notamment de la longueur, de la nature et des conditions de la présence de cette personne dans l'État d'émission, ou des liens familiaux ou économiques entre cette personne et cet État membre. Un véhicule immatriculé, un compte bancaire, le caractère ininterrompu du séjour de la personne dans l'État d'émission ou d'autres facteurs objectifs pourraient être pertinents pour établir qu'il existe des motifs raisonnables de croire que la personne concernée réside dans l'État d'émission. Une brève visite, des vacances, y compris dans une maison de vacances, ou un séjour similaire dans l'État d'émission, sans autre lien substantiel, ne suffit pas pour l'établissement d'une résidence dans cet État membre. Dans les cas où, au moment d'émettre une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou visant à obtenir des données relatives au contenu, l'autorité d'émission n'a pas de motifs raisonnables de croire que la personne dont les données sont demandées réside dans l'État d'émission, l'autorité d'émission devrait adresser une notification à l'autorité chargée de la mise en œuvre.

(54) Afin de garantir une procédure rapide, le moment à prendre en compte pour déterminer s'il y a lieu d'adresser une notification à l'autorité chargée de la mise en œuvre devrait être le moment où l'injonction européenne de production est émise. Tout changement ultérieur de résidence ne devrait avoir aucune incidence sur la procédure. La personne concernée devrait avoir la possibilité d'invoquer ses droits ainsi que les règles relatives à la détermination et à la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias, tout au long de la procédure pénale, et l'autorité chargée de la mise en œuvre devrait avoir la possibilité d'invoquer un motif de refus lorsque, dans des situations exceptionnelles, il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte. En outre, il devrait également être possible d'invoquer ces motifs pendant la procédure de mise en œuvre.

(55) Une injonction européenne de production devrait être transmise au moyen d'un EPOC, et une injonction européenne de conservation devrait être transmise au moyen d'un EPOC-PR. S'il y a lieu, l'EPOC ou l'EPOC-PR devrait être traduit dans une langue officielle de l'Union acceptée par le destinataire. Si aucune langue n'a été spécifiée par le fournisseur de services, l'EPOC ou l'EPOC-PR devrait être traduit dans une langue officielle de l'État membre dans lequel est situé l'établissement désigné ou le représentant légal du fournisseur de services, ou dans une autre langue officielle que l'établissement désigné ou le représentant légal du fournisseur de services a déclaré accepter. Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu du présent règlement, l'EPOC à transmettre à cette autorité devrait être traduit dans une langue officielle de l'État chargé de la mise en œuvre ou dans une autre langue officielle de l'Union acceptée par cet État. À cet égard, chaque État membre devrait être encouragé à indiquer, à tout moment, au moyen d'une déclaration écrite adressée à la Commission, s'il accepte que les EPOC et les EPOC-PR soient traduits, et dans quelle ou quelles langues officielles de l'Union ils doivent l'être, en plus de la ou des langues officielles dudit État membre. La Commission devrait mettre ces déclarations à la disposition de tous les États membres et du réseau judiciaire européen.

(56) Lorsqu'un EPOC a été émis et qu'une notification à l'autorité chargée de la mise en œuvre n'est pas requise en vertu du présent règlement, le destinataire devrait, dès réception de l'EPOC, s'assurer que les données demandées sont transmises directement à l'autorité d'émission ou aux autorités répressives, comme indiqué dans l'EPOC, au plus tard dans un délai de dix jours suivant la réception de l'EPOC. Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu du présent règlement, le fournisseur de services devrait, dès réception de l'EPOC, agir rapidement pour conserver les données. Lorsque l'autorité chargée de la mise en

œuvre n'a invoqué aucun motif de refus en vertu du présent règlement dans un délai de dix jours suivant la réception de l'EPOC, le destinataire devrait s'assurer que les données demandées sont transmises directement à l'autorité d'émission ou aux autorités répressives, comme indiqué dans l'EPOC, à l'expiration de ce délai de dix jours. Lorsque l'autorité chargée de la mise en œuvre, avant même l'expiration du délai de dix jours, confirme à l'autorité d'émission et au destinataire qu'elle n'invoquera aucun motif de refus, le destinataire devrait agir dès que possible après cette confirmation et au plus tard à l'expiration de ce délai de dix jours. Les délais plus courts applicables dans les cas d'urgence tels qu'ils sont définis dans le présent règlement devraient être respectés par le destinataire et, s'il y a lieu, par l'autorité chargée de la mise en œuvre. Le destinataire et, s'il y a lieu, l'autorité chargée de la mise en œuvre devraient exécuter l'EPOC dès que possible et au plus tard dans les délais fixés par le présent règlement, en tenant compte le plus possible des délais de procédure et des autres délais indiqués par l'État d'émission.

(57) Si le destinataire estime, sur la seule base des informations contenues dans l'EPOC ou dans l'EPOC-PR, que l'exécution de l'EPOC ou de l'EPOC-PR pourrait interférer avec les immunités ou privilèges, ou avec les règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, en vertu du droit de l'État d'exécution, il devrait en informer l'autorité d'émission et l'autorité chargée de la mise en œuvre. En ce qui concerne les EPOC, lorsqu'aucune notification à l'autorité chargée de la mise en œuvre n'a eu lieu en vertu du présent règlement, l'autorité d'émission devrait tenir compte des informations reçues du destinataire et devrait décider, de sa propre initiative ou à la demande de l'autorité chargée de la mise en œuvre, s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction européenne de production. Lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu du présent règlement, l'autorité d'émission devrait tenir compte des informations reçues du destinataire et décider s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction européenne de production. L'autorité chargée de la mise en œuvre devrait également avoir la possibilité d'invoquer les motifs de refus énoncés dans le présent règlement.

(58) Afin de permettre au destinataire de résoudre des problèmes formels liés à un EPOC ou à un EPOC-PR, il est nécessaire de définir une procédure pour la communication entre le destinataire et l'autorité d'émission et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu du présent règlement, entre le destinataire et l'autorité chargée de la mise en œuvre, dans les cas où l'EPOC ou l'EPOC-PR est incomplet ou contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour l'exécution de l'injonction concernée. Par ailleurs, si le destinataire ne fournit pas les informations de manière exhaustive ou en temps opportun pour toute autre raison, par exemple parce qu'il considère qu'il existe un conflit vis-à-vis d'une obligation relevant du droit d'un pays tiers, ou que l'injonction européenne de production ou l'injonction européenne de conservation n'a pas été émise en conformité avec les conditions prévues par le présent règlement, il devrait en informer l'autorité d'émission, et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu, l'autorité chargée de la mise en œuvre, et fournir la justification pour laquelle il ne peut donner suite à l'EPOC ou à l'EPOC-PR en temps opportun. La procédure de communication devrait donc permettre la correction ou le réexamen de l'injonction européenne de production ou de l'injonction européenne de conservation par l'autorité d'émission à un stade précoce. Pour garantir la disponibilité des données demandées, le destinataire devrait conserver ces données s'il peut identifier lesdites données.

(59) Le destinataire ne devrait pas être obligé de se conformer à l'injonction européenne de production ou à l'injonction européenne de conservation en cas d'impossibilité de fait en raison de circonstances qui ne lui sont pas imputables ou, lorsqu'il s'agit de personnes différentes, qui ne sont pas imputables au fournisseur de services au moment de la réception de l'injonction européenne de production ou de l'injonction européenne de conservation. Il y a lieu de présumer une impossibilité de fait lorsque la personne dont les données ont été demandées n'est pas un client du fournisseur de services ou ne peut pas être identifiée en tant que tel même après qu'une demande d'informations complémentaires a été adressée à l'autorité d'émission, ou si les données ont été supprimées légalement avant la réception de l'injonction concernée.

(60) Lorsqu'il reçoit un EPOC-PR, le destinataire devrait conserver les données demandées pendant soixante jours au maximum, sauf si l'autorité d'émission confirme qu'une demande de production ultérieure a été émise, auquel cas la conservation devrait être poursuivie. L'autorité d'émission devrait pouvoir prolonger la durée de conservation de trente jours supplémentaires, le cas échéant, pour permettre qu'une demande de production ultérieure soit émise, au moyen du formulaire figurant dans le présent règlement. Si l'autorité d'émission confirme, au cours de la période de conservation, qu'une demande de production ultérieure a été émise, le destinataire devrait conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande de production ultérieure aura été reçue. Cette confirmation devrait être envoyée au destinataire dans le délai imparti, dans une langue officielle de l'État chargé de la mise en œuvre ou dans toute autre langue acceptée par le destinataire, au moyen du formulaire figurant dans le présent règlement. Pour éviter que la conservation cesse, il devrait suffire que la demande de production ultérieure ait été émise et que la confirmation ait été envoyée par l'autorité d'émission; il ne devrait pas être nécessaire, à ce stade, d'accomplir d'autres formalités requises pour la transmission, telles que la traduction des documents. Lorsque la conservation n'est plus nécessaire, l'autorité d'émission devrait en informer le destinataire sans retard injustifié et l'obligation de conservation fondée sur l'injonction européenne de conservation devrait prendre fin.

(61) Nonobstant le principe de confiance mutuelle, l'autorité chargée de la mise en œuvre doit pouvoir invoquer des motifs de refus d'une injonction européenne de production, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu du présent règlement, sur la base de la liste des motifs de refus prévue par le présent règlement. Lorsqu'une notification à l'autorité chargée de la mise en œuvre ou que la mise en œuvre elle-même a lieu conformément au présent règlement, l'État membre chargé de la mise en œuvre pourrait prévoir, dans son droit national, que l'exécution d'une injonction européenne de production pourrait nécessiter l'intervention procédurale d'une juridiction de l'État chargé de la mise en œuvre.

(62) Lorsque l'autorité chargée de la mise en œuvre a reçu notification d'une injonction européenne de production en vue d'obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies dans le présent règlement, ou d'obtenir des données relatives au contenu, elle devrait avoir le droit d'évaluer les informations figurant dans l'injonction et, le cas échéant, de refuser l'injonction lorsque, sur la base d'une analyse obligatoire et appropriée des informations contenues dans cette injonction et dans le respect des règles applicables du droit primaire de l'Union, en particulier de la Charte, elle parvient à la conclusion qu'un ou plusieurs des motifs de refus prévus par le présent règlement pourraient être invoqués. La nécessité de respecter l'indépendance des autorités judiciaires exige qu'une certaine marge d'appréciation soit accordée à ces autorités lorsqu'elles prennent des décisions concernant les motifs de refus.

(63) L'autorité chargée de la mise en œuvre devrait avoir la possibilité, lorsqu'une notification lui est adressée en vertu du présent règlement, de refuser une injonction européenne de production lorsque les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre qui empêchent l'exécution ou la mise en œuvre de l'injonction européenne de production, ou lorsque les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction européenne de production.

(64) L'autorité chargée de la mise en œuvre devrait avoir la possibilité de refuser une injonction, dans des situations exceptionnelles, lorsqu'il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction européenne de production entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte. En particulier, lorsqu'elle évalue ce motif de refus, lorsque l'autorité chargée de la mise en œuvre dispose de preuves ou d'éléments tels que ceux énoncés dans une proposition motivée émanant d'un tiers des États membres, du Parlement européen ou de la Commission européenne, adoptée en vertu de l'article 7, paragraphe 1, du traité sur l'Union européenne, indiquant qu'il existe un risque manifeste, si l'injonction était exécutée, d'une violation grave du droit fondamental à un recours effectif et à un procès équitable prévus à l'article 47 de la Charte, en raison de défaillances systémiques ou généralisées en ce qui concerne l'indépendance du pouvoir judiciaire de l'État d'émission, l'autorité chargée de la mise en œuvre devrait déterminer concrètement et précisément si, compte tenu de la situation personnelle de la personne concernée, ainsi que de la nature de l'infraction pour laquelle la procédure pénale est menée et du contexte factuel qui constitue le fondement de l'injonction, et à la lumière des informations fournies par l'autorité d'émission, il existe des motifs sérieux de croire qu'il existe un risque de violation du droit d'une personne à un procès équitable.

(65) L'autorité chargée de la mise en œuvre devrait avoir la possibilité de refuser une injonction lorsque son exécution est contraire au principe ne bis in idem.

(66) L'autorité chargée de la mise en œuvre devrait avoir la possibilité, lorsqu'une notification lui est adressée en vertu du présent règlement, de refuser une injonction européenne de production lorsque les faits pour lesquels l'injonction a été émise ne constituent pas une infraction au titre du droit de l'État chargé de la mise en œuvre, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions énumérées dans une annexe du présent règlement, 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 privatives de liberté d'une durée maximale d'au moins trois ans.

(67) Étant donné qu'informer la personne dont les données sont demandées constitue un élément essentiel en ce qui concerne les droits en matière de protection des données et les droits de la défense, dans la mesure où elle permet un contrôle effectif et un recours juridictionnel, conformément à l'article 6 du traité sur l'Union européenne et à la Charte, l'autorité d'émission devrait informer, sans retard injustifié, la personne dont les données sont demandées de la production des données fondée sur une injonction européenne de production. Toutefois, l'autorité d'émission devrait être en mesure, conformément au droit national, de retarder ou de limiter l'information de la personne dont les données sont demandées, voire de ne pas l'informer, dans la mesure où et aussi longtemps que les conditions de la directive (UE) 2016/680 sont remplies, auquel cas l'autorité d'émission devrait indiquer dans le dossier les raisons du retard ou de la limitation de l'information, ou de la non-information, et ajouter une brève justification dans l'EPOC. Les destinataires et, lorsqu'il s'agit de personnes différentes, les fournisseurs de services devraient prendre 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.

(68) Un fournisseur de services devrait pouvoir demander à l'État d'émission le remboursement des coûts qu'il a engagés pour répondre à une injonction européenne de production ou à une injonction européenne de conservation, si cette possibilité est prévue dans le droit national de l'État d'émission pour des injonctions nationales dans des situations similaires, conformément au droit national de cet État. Les États membres devraient communiquer leurs règles nationales en matière de remboursement à la Commission, qui devrait les rendre publiques. Le présent règlement prévoit des règles distinctes applicables au remboursement des coûts liés au système informatique décentralisé.

(69) Sans préjudice de leur droit national prévoyant d'imposer des sanctions pénales, les États membres devraient déterminer le régime relatif aux sanctions pécuniaires applicables en cas d'infractions au présent règlement et prendre toutes les mesures nécessaires pour garantir la mise en œuvre de ces sanctions. Les États membres devraient veiller à ce que les sanctions pécuniaires prévues dans leur droit national soient effectives, proportionnées et dissuasives. Les États membres devraient notifier, sans retard, ces règles et mesures à la Commission et l'informer, sans retard, de toute modification ultérieure les concernant.

(70) Lorsqu'elles évaluent, dans un cas d'espèce, les sanctions pécuniaires appropriées, les autorités compétentes devraient tenir compte de toutes les circonstances pertinentes, telles que la nature, la gravité et la durée de l'infraction, le fait qu'elle ait été commise intentionnellement ou par négligence, le fait que le fournisseur de services ait déjà été tenu responsable d'infractions similaires et la solidité financière du fournisseur de services tenu responsable. Dans des circonstances exceptionnelles, cette évaluation pourrait conduire l'autorité chargée de la mise en œuvre à décider de s'abstenir d'imposer des sanctions pécuniaires. À cet égard, une attention particulière doit être accordée aux microentreprises qui manquent de se conformer à une injonction européenne de production ou à une injonction européenne de conservation dans un cas d'urgence en raison du manque de ressources humaines en dehors des heures normales de bureau, si les données sont transmises sans retard injustifié.

(71) Sans préjudice des obligations en matière de protection des données, les fournisseurs de services ne devraient pas être tenus responsables dans les États membres du préjudice causé à leurs utilisateurs ou à des tiers résultant exclusivement du respect de bonne foi d'un EPOC ou d'un EPOC-PR. Il devrait incomber à l'autorité d'émission de garantir la légalité de l'injonction concernée, en particulier de sa nécessité et de sa proportionnalité.

(72) Lorsque le destinataire ne respecte pas un EPOC dans les délais impartis ou un EPOC-PR, sans fournir de raisons acceptées par l'autorité d'émission, et, le cas échéant, lorsque l'autorité chargée de la mise en œuvre n'a invoqué aucun des motifs de refus énumérés dans le présent règlement, l'autorité d'émission devrait pouvoir demander à l'autorité chargée de la mise en œuvre de mettre en œuvre l'injonction européenne de production ou l'injonction européenne de conservation. À cette fin, l'autorité d'émission devrait transférer à l'autorité chargée de la mise en œuvre l'injonction concernée, le formulaire pertinent prévu par le présent règlement complété par le destinataire, ainsi que tout document pertinent. L'autorité d'émission devrait traduire l'injonction concernée et tout document qui doit être transféré dans l'une des langues acceptées par l'État chargé de la mise en œuvre et devrait informer le destinataire du transfert. Cet État membre devrait mettre en œuvre l'injonction concernée conformément à son droit national.

(73) La procédure de mise en œuvre devrait permettre au destinataire d'invoquer des motifs à l'encontre de la mise en œuvre sur la base d'une liste de motifs spécifiques prévus par le présent règlement, y compris le fait que l'injonction concernée n'a pas été émise ou validée par une autorité compétente comme le prévoit le présent règlement, ou lorsque l'injonction ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception du certificat correspondant. L'autorité chargée de la mise en œuvre devrait pouvoir refuser de reconnaître et de mettre en œuvre une injonction européenne de production ou une injonction européenne de conservation basée sur ces mêmes motifs, ainsi que, dans des situations exceptionnelles, en raison de la violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte. L'autorité chargée de la mise en œuvre devrait consulter l'autorité d'émission avant de décider de ne pas reconnaître ou de ne pas mettre en œuvre l'injonction sur la base de ces motifs. Lorsque le destinataire ne respecte pas les obligations qui lui incombent en vertu d'une injonction européenne de production ou d'une injonction européenne de conservation reconnues, dont le caractère exécutoire a été confirmé par l'autorité chargée de la mise en œuvre, cette autorité devrait imposer une sanction pécuniaire. Cette sanction devrait être proportionnée, compte tenu, en particulier, des circonstances spécifiques telles qu'un manquement répété ou systématique.

(74) Le respect d'une injonction européenne de production pourrait entrer en conflit avec une obligation prévue par le droit applicable d'un pays tiers. Par courtoisie envers les intérêts souverains des pays tiers, et afin de protéger les personnes concernées et de concilier les obligations en conflit des fournisseurs de services, le présent règlement prévoit un mécanisme spécifique de contrôle juridictionnel lorsque le respect d'une injonction européenne de production empêcherait un fournisseur de services de respecter les obligations légales découlant du droit d'un pays tiers.

(75) Lorsqu'un destinataire considère que, dans un cas spécifique, une injonction européenne de production entraînerait la violation d'une obligation légale découlant du droit d'un pays tiers, il devrait informer l'autorité d'émission et l'autorité chargée de la mise en œuvre des raisons pour lesquelles il ne peut exécuter l'injonction par la voie d'une objection motivée, au moyen du formulaire prévu par le présent règlement. L'autorité d'émission devrait examiner l'injonction européenne de production sur la base de l'objection motivée et de toute contribution apportée par l'État chargé de la mise en œuvre, en tenant compte des mêmes critères que ceux que la juridiction compétente de l'État d'émission devrait suivre. Lorsque l'autorité d'émission a l'intention de maintenir l'injonction, elle devrait demander un réexamen par la juridiction compétente de l'État d'émission, qui a fait l'objet d'une notification par l'État membre concerné, qui devrait réexaminer l'injonction.

(76) Pour déterminer l'existence d'une obligation en conflit dans les circonstances spécifiques de l'affaire examinée, la juridiction compétente pourrait s'appuyer sur une expertise externe appropriée si nécessaire, par exemple sur l'interprétation du droit du pays tiers concerné. À cet effet, la juridiction compétente pourrait, par exemple, consulter l'autorité centrale du pays tiers, en tenant compte de la directive (UE) 2016/680. L'État d'émission devrait notamment demander des informations à l'autorité compétente du pays tiers lorsque le conflit concerne des droits fondamentaux ou d'autres intérêts fondamentaux du pays tiers liés à la sécurité et à la défense nationales.

(77) Une expertise sur l'interprétation pourrait également être fournie par le biais d'avis d'experts lorsqu'ils sont disponibles. Les informations et la jurisprudence sur l'interprétation du droit 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 ou le réseau judiciaire européen, afin de pouvoir bénéficier de l'expérience et de l'expertise acquises sur des questions identiques ou similaires. La disponibilité de ces informations sur une plateforme centrale ne devrait pas empêcher une nouvelle consultation du pays tiers le cas échéant.

(78) Lorsqu'elle évalue s'il existe des obligations en conflit, la juridiction compétente devrait déterminer si le droit du pays tiers est applicable et, dans l'affirmative, si le droit du pays tiers interdit la divulgation des données concernées. Lorsque la juridiction compétente établit que le droit du pays tiers interdit la divulgation des données concernées, cette juridiction devrait décider s'il y a lieu de maintenir ou de lever l'injonction européenne de production, en pondérant un certain nombre d'éléments visant à déterminer la force de la connexion à l'une ou l'autre des deux juridictions concernées, les intérêts respectifs à obtenir ou, au contraire, à empêcher la divulgation des données, et les éventuelles conséquences pour le destinataire ou le fournisseur de services du respect de l'injonction. Il convient, lors de l'évaluation, d'accorder une importance particulière et un poids particulier à la protection des droits fondamentaux par la disposition de droit pertinente du pays tiers et d'autres intérêts fondamentaux, tels les intérêts liés à la sécurité nationale du pays tiers, ainsi que le degré de connexion de l'affaire pénale avec l'une ou l'autre des deux juridictions. Lorsque la juridiction décide de lever l'injonction, elle devrait en informer l'autorité d'émission et le destinataire. Si la juridiction compétente décide que l'injonction doit être maintenue, elle devrait en informer l'autorité d'émission et le destinataire, lequel devrait procéder à l'exécution de cette injonction. L'autorité d'émission devrait informer l'autorité chargée de la mise en œuvre du résultat de la procédure de réexamen.

(79) Les conditions énoncées dans le présent règlement en ce qui concerne l'exécution d'un EPOC devraient également être applicables en cas d'obligations en conflit découlant du droit d'un pays tiers. Par conséquent, lors du contrôle juridictionnel, lorsque le respect d'une injonction européenne de production empêcherait les fournisseurs de services de respecter une obligation légale découlant du droit d'un pays tiers, les données demandées par cette injonction devraient être conservées. Lorsque, à la suite du contrôle juridictionnel, la juridiction compétente décide de lever une injonction européenne de production, il devrait être possible d'émettre une injonction européenne de conservation pour permettre à l'autorité d'émission de requérir la production des données par d'autres canaux tels que l'entraide judiciaire.

(80) Il est essentiel que toutes les personnes dont les données sont demandées dans le cadre d'enquêtes ou de procédures pénales aient accès à un recours juridictionnel effectif, conformément à l'article 47 de la Charte. Dans le respect de cette exigence et sans préjudice d'autres recours légaux disponibles conformément au droit national, toute personne dont les données ont été demandées au moyen d'une injonction européenne de production devrait avoir droit à des recours effectifs contre cette injonction. Lorsque cette personne est un suspect ou une personne poursuivie, celle-ci devrait avoir droit à des recours effectifs pendant la procédure pénale au cours de laquelle les données sont utilisées comme preuve. Le droit à des recours effectifs devrait être exercé devant une juridiction de l'État d'émission conformément à son droit national et devrait comprendre la possibilité de contester la légalité de la mesure, notamment sa nécessité et sa proportionnalité, sans préjudice des garanties des droits fondamentaux dans l'État chargé de la mise en œuvre ou d'autres voies de recours supplémentaires prévues par le droit national. Le présent règlement ne devrait pas limiter les motifs possibles de contestation de la légalité d'une injonction. Le droit à des recours effectifs prévu par le présent règlement devrait être sans préjudice du droit de former un recours prévu par le règlement (UE) 2016/679 et la directive (UE) 2016/680. Il convient de fournir en temps utile des informations sur les possibilités de former un recours prévues par le droit national et de veiller à ce que ces recours soient exercés de manière effective.

(81) Des canaux appropriés devraient être mis en place pour garantir que toutes les parties puissent coopérer efficacement par des moyens numériques, grâce à un système informatique décentralisé permettant l'échange électronique transfrontière rapide, direct, interopérable, durable, fiable et sécurisé de formulaires, de données et d'informations liés aux affaires.

(82) Afin de permettre une communication écrite efficace et sécurisée entre les autorités compétentes et les établissements désignés ou les représentants légaux des fournisseurs de services au titre du présent règlement, ces établissements désignés ou ces représentants légaux devraient disposer de moyens électroniques d'accès aux systèmes informatiques nationaux, qui font partie du système informatique décentralisé, gérés par les États membres.

(83) Le système informatique décentralisé devrait comprendre les systèmes informatiques des États membres et des agences et organes de l'Union, ainsi que des points d'accès interopérables, par l'intermédiaire desquels ces systèmes informatiques sont interconnectés. Les points d'accès du système informatique décentralisé devrait se fonder sur le système e-CODEX, établi par le règlement (UE) 2022/850 du Parlement européen et du Conseil ([24]).

(84) Les fournisseurs de services qui utilisent des solutions informatiques sur mesure aux fins de l'échange d'informations et de données liées aux demandes de preuves électroniques devraient disposer de moyens automatisés pour accéder aux systèmes informatiques décentralisés grâce à une norme commune en matière d'échange de données.

(85) En principe, toutes les communications écrites entre les autorités compétentes ou entre les autorités compétentes et les établissements désignés ou les représentants légaux devraient passer par le système informatique décentralisé. Des moyens de substitution ne devraient pouvoir être utilisés que lorsqu'il n'est pas possible d'utiliser le système informatique décentralisé, notamment parce qu'il existe des exigences médico-légales spécifiques, parce que le volume de données ne peut être transféré correctement du fait de contraintes en matière de capacité technique ou parce qu'un autre établissement non connecté au système informatique décentralisé doit être contacté dans un cas d'urgence. En pareils cas, la transmission devrait être effectuée par les moyens de substitution les plus appropriés, en tenant compte de la nécessité de garantir un échange d'informations rapide, sécurisé et fiable.

(86) Afin de s'assurer que le système informatique décentralisé comporte un enregistrement exhaustif des échanges écrits, comme le prévoit le présent règlement, toute transmission effectuée par des moyens de substitution devrait être enregistrée sans retard injustifié dans le système informatique décentralisé.

(87) L'utilisation de mécanismes garantissant l'authenticité devrait être envisagée, comme le prévoit le règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([25]).

(88) Les fournisseurs de services, en particulier les petites et moyennes entreprises, ne devraient pas être exposés à des coûts disproportionnés en ce qui concerne la mise en place et le fonctionnement du système informatique décentralisé. Dans le cadre de la création, de l'entretien et du développement de la mise en œuvre de référence, la Commission doit donc également mettre à disposition une interface internet permettant aux fournisseurs de services de communiquer en toute sécurité avec les autorités sans avoir à mettre en place leur propre infrastructure spécifique pour accéder au système informatique décentralisé.

(89) Les États membres devraient pouvoir utiliser le logiciel développé par la Commission, à savoir le logiciel de mise en œuvre de référence, en lieu et place d'un système informatique national. Ce logiciel de mise en œuvre de référence doit être basé sur une configuration modulaire, ce qui signifie que le logiciel est conditionné et livré séparément des composants du système e-CODEX nécessaires pour le connecter au système informatique décentralisé. Cette configuration devrait permettre aux États membres de réutiliser ou d'améliorer leurs infrastructures nationales de communication judiciaire respectives existantes à des fins d'utilisation transfrontière.

(90) La Commission devrait être responsable de la création, de la maintenance et du développement du logiciel de mise en œuvre de référence. La Commission devrait concevoir et développer le logiciel de mise en œuvre de référence et en assurer la maintenance dans le respect des exigences et principes en matière de protection des données fixés dans le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([26]), le règlement (UE) 2016/679 et la directive (UE) 2016/680, en particulier les principes de protection des données dès la conception et par défaut, et la garantie d'un niveau élevé de cybersécurité. Il importe que le logiciel de mise en œuvre de référence comporte également des mesures techniques appropriées et permette de prendre les mesures organisationnelles nécessaires pour assurer un niveau approprié de sécurité et d'interopérabilité.

([24]) Règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-CODEX), et modifiant le règlement (UE) 2018/1726 (JO L 150 du 1.6.2022, p. 1).

([25]) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

([26]) 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).

(91) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([27]).

(92) En ce qui concerne les échanges de données effectués au moyen du système informatique décentralisé ou enregistrés dans le système informatique décentralisé, les États membres devraient être en mesure de collecter des statistiques afin de remplir leurs obligations en matière de suivi et de communication d'informations au titre du présent règlement par l'intermédiaire de leurs portails nationaux.

(93) Afin d'assurer le suivi des réalisations, des résultats et des incidences du présent règlement, la Commission devrait publier un rapport annuel portant sur l'année civile précédente, à partir des données obtenues auprès des États membres. À cette fin, les États membres devraient collecter et fournir à la Commission des statistiques complètes sur les différents aspects du présent règlement, par type de données demandées et par destinataire, et indiquer s'il s'agissait ou non d'un cas d'urgence.

(94) L'utilisation de formulaires prétraduits et standardisés pourrait faciliter la coopération et l'échange d'informations au titre du présent règlement, permettant ainsi de communiquer plus rapidement et plus efficacement d'une manière conviviale. Ces formulaires pourraient réduire les coûts de traduction et contribuer à une norme de qualité élevée en matière de communication. Les formulaires de réponse pourraient rendre possible un échange d'informations normalisé, en particulier lorsque les fournisseurs de services ne peuvent pas se conformer à une demande parce que le compte d'utilisateur n'existe pas ou parce qu'aucune donnée n'est disponible. Les formulaires prévus par le présent règlement pourraient faciliter également la collecte de statistiques.

(95) Afin de répondre efficacement à un éventuel besoin d'améliorations concernant le contenu des formulaires EPOC et EPOC-PR ainsi que des formulaires à utiliser pour fournir des informations sur l'impossibilité d'exécuter un EPOC ou un EPOC-PR, pour confirmer l'émission d'une demande de production à la suite d'une injonction européenne de conservation et pour prolonger la conservation des preuve électroniques, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne la modification des formulaires prévus par le présent règlement. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer» ([28]). En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(96) Le présent règlement ne devrait pas porter atteinte aux instruments, conventions et accords de l'Union ou à d'autres instruments, conventions et accords internationaux relatifs à l'obtention de preuves qui relève du champ d'application du présent règlement. Les autorités des États membres devraient choisir l'outil le plus adapté au cas d'espèce. Dans certains cas, elles pourraient privilégier l'utilisation d'instruments, de conventions et d'accords de l'Union ou d'autres instruments, conventions et accords internationaux pour demander à un autre État membre un ensemble de différents types de mesures d'enquête qui ne se limitent pas à la production de preuves électroniques. Les États membres devraient notifier à la Commission, au plus tard trois ans après l'entrée en vigueur du présent règlement, les instruments, conventions et accords existants, visés dans le présent règlement, qu'ils continueront d'appliquer. Les États membres notifient également à la Commission, dans un délai de trois mois à compter de leur signature, toute nouvelle convention ou tout nouvel accord visé dans le présent règlement.

(97) Compte tenu des évolutions technologiques, de nouvelles formes d'outils de communication pourraient s'imposer dans quelques années, ou des lacunes pourraient apparaître dans l'application du présent règlement. Il est de ce fait important de prévoir une évaluation de son application.

(98) La Commission devrait procéder à une évaluation du présent règlement fondée sur les cinq critères d'efficience, d'efficacité, de pertinence, de cohérence et de valeur ajoutée de l'UE et cette évaluation devrait servir de base aux analyses d'impact d'éventuelles mesures supplémentaires. Le rapport d'évaluation devrait comporter une évaluation de l'application du présent règlement et des résultats obtenus en ce qui concerne ses objectifs, ainsi qu'une évaluation de l'incidence du présent règlement sur les droits fondamentaux. La Commission devrait collecter les informations régulièrement dans le but d'alimenter l'évaluation du présent règlement.

([27]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

([28]) JO L 123 du 12.5.2016, p. 1.

(99) Étant donné que l'objectif du présent règlement, à savoir améliorer la collecte et l'obtention de preuves électroniques par-delà les frontières, ne peut pas être atteint de manière suffisante par les États membres en raison de son caractère transfrontière, mais peut l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(100) Conformément à l'article 3 du protocole n° 21 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.

(101) Conformément aux articles 1er 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 ni soumis à son application.

(102) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a émis un avis le 6 novembre 2019 ([29]),

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

CHAPITRE I

OBJET, CHAMP D'APPLICATION ET DÉFINITIONS

Article premier

Objet

1. Le présent règlement définit les règles selon lesquelles, dans le cadre de procédures pénales, une autorité d'un État membre peut émettre une injonction européenne de production ou une injonction européenne de conservation et, partant, ordonner à un fournisseur de services proposant des services dans l'Union et établi dans un autre État membre ou, s'il n'y est pas établi, représenté par un représentant légal dans un autre État membre, de produire ou de conserver des preuves électroniques, quelle que soit la localisation des données.

Le présent règlement est sans préjudice des pouvoirs des autorités nationales de s'adresser aux fournisseurs de services établis ou représentés sur leur territoire afin de s'assurer qu'ils respectent des mesures nationales similaires à celles visées au premier alinéa.

2. Dans le cadre des droits de la défense applicables conformément au droit national en matière de procédure pénale, l'émission d'une injonction européenne de production ou d'une injonction européenne de conservation peut également être demandée par un suspect ou une personne poursuivie ou par un avocat agissant au nom de cette personne.

3. 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, et toute obligation applicable aux autorités répressives ou aux autorités judiciaires à cet égard demeure inchangée. Le présent règlement s'applique sans préjudice des principes fondamentaux, en particulier la liberté d'expression et d'information, notamment la liberté et le pluralisme des médias, le respect de la vie privée et familiale, la protection des données à caractère personnel, ainsi que le droit à une protection juridictionnelle effective.

Article 2

Champ d'application

1. Le présent règlement s'applique aux fournisseurs de services qui proposent des services dans l'Union.

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 et aux fins de l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois prononcées, à l'issue de procédures pénales, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice. Ces injonctions peuvent également être émises dans des procédures relatives à une infraction pénale pour laquelle une personne morale pourrait être tenue responsable ou sanctionnée dans l'État d'émission.

3. Les injonctions européennes de production et les injonctions européennes de conservation ne peuvent être émises que pour les données relatives aux services visés à l'article 3, point 3), proposés dans l'Union.

4. Le présent règlement ne s'applique pas aux procédures engagées en vue de fournir une entraide judiciaire à un autre État membre ou à un pays tiers.

([29]) JO C 32 du 31.1.2020, p. 11.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «injonction européenne de production»: une décision ordonnant la production de preuves électroniques, émise ou validée par une autorité judiciaire d'un État membre conformément à l'article 4, paragraphes 1, 2, 4 et 5, et adressée à un établissement désigné ou à un représentant légal d'un fournisseur de services proposant des services dans l'Union, lorsque cet établissement désigné ou ce représentant légal est situé dans un autre État membre lié par le présent règlement;

2) «injonction européenne de conservation»: une décision qui ordonne la conservation de preuves électroniques aux fins d'une demande de production ultérieure, et qui est émise ou validée par une autorité judiciaire d'un État membre conformément à l'article 4, paragraphes 3, 4 et 5, et adressée à un établissement désigné ou à un représentant légal d'un fournisseur de services proposant des services dans l'Union, lorsque cet établissement désigné ou ce représentant légal est situé dans un autre État membre lié par le présent règlement;

3) «fournisseur de services»: toute personne physique ou morale qui fournit une ou plusieurs des catégories de services suivantes, à l'exception des services financiers visés à l'article 2, paragraphe 2, point b), de la directive 2006/123/CE du Parlement européen et du Conseil ([30]):

   a) des services de communications électroniques tels qu'ils sont définis à l'article 2, point 4), de la directive (UE) 2018/1972;

   b) des services d'attribution de noms de domaine sur l'internet et de numérotation IP, tels que l'attribution d'adresses IP, les services du registre de noms de domaine, les services du bureau d'enregistrement de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire liés aux noms de domaine;

   c) d'autres services de la société de l'information visés à l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 qui:

      i) permettent à leurs utilisateurs de communiquer entre eux; ou

      ii) permettent de stocker ou de traiter d'une autre manière des données pour le compte des utilisateurs auxquels le service est fourni, à condition que le stockage des données soit une composante déterminante du service fourni à l'utilisateur;

4) «proposer des services dans l'Union»:

   a) permettre aux personnes physiques ou morales dans un État membre d'utiliser les services énumérés au point 3); et

   b) avoir un lien substantiel, fondé sur des critères factuels spécifiques, avec l'État membre visé au point a); un tel lien substantiel est réputé exister lorsque le fournisseur de services dispose d'un établissement dans un État membre ou, en l'absence d'un tel établissement, lorsqu'il existe un nombre significatif d'utilisateurs dans un ou plusieurs États membres ou lorsqu'il existe un ciblage des activités sur un ou plusieurs États membres;

5) «établissement»: une entité qui exerce de manière effective une activité économique pendant une durée indéterminée au moyen d'une infrastructure stable à partir de laquelle l'activité de fourniture de services est réalisée ou à partir de laquelle l'activité est gérée;

6) «établissement désigné»: un établissement doté de la personnalité juridique désigné par écrit par un fournisseur de services qui est établi dans un État membre participant à un instrument juridique visé à l'article 1er, paragraphe 2, de la directive (UE) 2023/1544, aux fins visées à l'article 1er, paragraphe 1, et à l'article 3, paragraphe 1, de ladite directive;

7) «représentant légal»: une personne physique ou morale désignée par écrit par un fournisseur de services qui n'est pas établi dans un État membre participant à un instrument juridique visé à l'article 1er, paragraphe 2, de la directive (UE) 2023/1544, aux fins visées à l'article 1er, paragraphe 1, et à l'article 3, paragraphe 1, de ladite directive;

8) «preuves électroniques»: les données relatives aux abonnés, les données relatives au trafic ou les données relatives au contenu stockées par un fournisseur de services ou pour le compte d'un fournisseur de services, sous une forme numérique, au moment de la réception d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR);

([30]) Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).

9) «données relatives aux abonnés»: toutes données détenues par un fournisseur de services concernant l'abonnement à ses services, relatives à:

a) l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis;

b) le type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques connexes ou les interfaces utilisées ou fournies par l'abonné ou le client au moment du premier enregistrement ou de la première activation, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou autres moyens d'authentification utilisés à la place d'un mot de passe qui sont fournis par un utilisateur ou créés à la demande d'un utilisateur;

10) «données demandées à la seule fin d'identifier l'utilisateur»: les adresses IP et, si nécessaire, les ports de provenance et l'horodatage pertinents, à savoir la date et l'heure, ou les équivalents techniques de ces identifiants et les informations connexes, lorsque les services répressifs ou les autorités judiciaires les demandent à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique;

11) «données relatives au trafic»: les données relatives à la fourniture d'un service proposé par un fournisseur de services qui servent à fournir des informations contextuelles ou supplémentaires sur ce service et qui sont générées ou traitées par un système d'information du fournisseur de services, tels que la source et la destination d'un message ou un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service;

12) «données relatives au contenu»: toutes données dans un format numérique telles 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;

13) «système d'information»: un système d'information tel qu'il est défini à l'article 2, point a), de la directive 2013/40/UE du Parlement européen et du Conseil ([31]);

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

15) «autorité d'émission»: l'autorité compétente de l'État d'émission qui, conformément à l'article 4, peut émettre une injonction européenne de production ou une injonction européenne de conservation;

16) «État chargé de la mise en œuvre»: l'État membre dans lequel l'établissement désigné est établi ou dans lequel le représentant légal réside et auquel une injonction européenne de production et un EPOC ou une injonction européenne de conservation et un EPOC-PR sont transmis par l'autorité d'émission à des fins de notification ou à des fins de mise en œuvre conformément au présent règlement;

17) «autorité chargée de la mise en œuvre»: l'autorité dans l'État chargé de la mise en œuvre qui, conformément au droit national de cet État, est compétente pour recevoir une injonction européenne de production et un EPOC ou une injonction européenne de conservation et un EPOC-PR transmis par l'autorité d'émission à des fins de notification ou à des fins de mise en œuvre conformément au présent règlement;

18) «cas d'urgence»: une situation dans laquelle il existe une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne ou pour une infrastructure critique, telle qu'elle est définie à l'article 2, point a), de la directive 2008/114/CE, lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice des fonctions essentielles de l'État;

19) «responsable du traitement»: le responsable du traitement tel qu'il est défini à l'article 4, point 7), du règlement (UE) 2016/679;

20) «sous-traitant»: le sous-traitant tel qu'il est défini à l'article 4, point 8), du règlement (UE) 2016/679;

([31]) 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).

21) «système informatique décentralisé»: un réseau de systèmes informatiques et de points d'accès interopérables, dont le fonctionnement relève de la responsabilité et de la gestion individuelles de chaque État membre, agence ou organe de l'Union, qui permet que l'échange d'informations transfrontière s'effectue d'une manière sécurisée et fiable.

CHAPITRE II

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 ou visant à obtenir des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ne peut être émise que par:

a) un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée; ou

b) toute autre autorité compétente définie par l'État d'émission qui, dans l'affaire concernée, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément au droit national; dans ce cas, l'injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production prévues dans le 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 visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou visant à obtenir des données relatives au contenu, ne peut être émise que par:

a) un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée; ou

b) toute autre autorité compétente définie par l'État d'émission qui, dans l'affaire concernée, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément au droit national; dans ce cas, l'injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production prévues dans le présent règlement, par un juge, une juridiction ou un juge d'instruction dans l'État d'émission.

3. Une injonction européenne de conservation concernant des données de toute catégorie ne peut être émise que par:

a) un juge, une juridiction, un juge d'instruction ou un procureur compétents dans l'affaire concernée; ou

b) toute autre autorité compétente définie par l'État d'émission qui, dans l'affaire concernée, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément au droit national; dans ce cas, l'injonction européenne de conservation est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de conservation prévues dans le présent règlement, par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

4. Lorsqu'une injonction européenne de production ou une injonction européenne de conservation a été validée par une autorité judiciaire en vertu du paragraphe 1, point b), du paragraphe 2, point b), ou du paragraphe 3, point b), cette autorité peut également être considérée comme une autorité d'émission aux fins de la transmission de l'EPOC et de l'EPOC-PR.

5. Dans un cas d'urgence dont l'existence est établie de manière valable, tel qu'il est défini à l'article 3, point 18), les autorités compétentes visées au paragraphe 1, point b), et au paragraphe 3, point b), du présent article peuvent, à titre exceptionnel, émettre une injonction européenne de production concernant les données relatives aux abonnés ou les données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou une injonction européenne de conservation sans validation préalable de l'injonction concernée, lorsque la validation ne peut pas être obtenue à temps et si ces autorités pourraient émettre une injonction sans validation préalable dans le cadre d'une procédure nationale similaire. L'autorité d'émission demande une validation ex post de l'injonction concernée sans retard injustifié, au plus tard dans les 48 heures. Lorsque cette validation ex post de l'injonction concernée n'est pas accordée, l'autorité d'émission retire immédiatement l'injonction et supprime ou limite d'une autre manière l'utilisation de toutes données qui ont été obtenues.

6. Chaque État membre peut désigner une ou plusieurs autorités centrales chargées de la transmission administrative des EPOC et des EPOC-PR, des injonctions européennes de production et des injonctions européennes de conservation, et des notifications et chargées de la réception des données et des notifications ainsi que de la transmission de toute autre correspondance officielle concernant ces certificats ou injonctions.

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. Une injonction européenne de production doit être nécessaire et proportionnée aux fins de la procédure visée à l'article 2, paragraphe 3, compte tenu des droits du suspect ou de la personne poursuivie, et ne peut être émise que si une injonction similaire aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire.

3. Une injonction européenne de production visant à obtenir des données relatives aux abonnés ou visant à obtenir des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), peut être émise pour toutes les infractions pénales et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois, prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

4. Une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du présent règlement ou visant à obtenir des données relatives au contenu, n'est émise que:

a) pour des infractions pénales punissables dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans; ou

b) pour les infractions suivantes, si elles sont totalement ou partiellement commises au moyen d'un système d'information:

   i) les infractions, telles qu'elles sont définies aux articles 3 à 8 de la directive (UE) 2019/713 du Parlement européen et du Conseil ([32]);

   ii) les infractions, telles qu'elles sont définies aux articles 3 à 7 de la directive 2011/93/UE;

   iii) les infractions, telles qu'elles sont définies aux articles 3 à 8 de la directive 2013/40/UE;

c) pour les infractions pénales définies aux articles 3 à 12 et à l'article 14 de la directive (UE) 2017/541;

d) pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois, prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice, pour les infractions pénales visées aux points a), b) et c) du présent paragraphe.

5. Une injonction européenne de production inclut les informations suivantes:

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

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

c) l'utilisateur, sauf si l'injonction a pour seule fin d'identifier l'utilisateur, ou tout autre identifiant unique tel que le nom d'utilisateur, l'identifiant de connexion ou le nom du compte afin de déterminer les données qui sont demandées;

d) la catégorie de données demandée telle qu'elle est définie à l'article 3, points 9) à 12);

e) s'il y a lieu, la période couverte par les données pour lesquelles la production est demandée;

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

g) dans les cas d'urgence, tels qu'ils sont définis à l'article 3, point 18), les raisons dûment justifiées de l'urgence;

h) dans les cas où l'injonction européenne de production est directement adressée au fournisseur de services qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement, une confirmation que les conditions énoncées au paragraphe 6 du présent article sont remplies;

i) les motifs qui permettent d'établir que l'injonction européenne de production remplit les conditions de nécessité et de proportionnalité visées au paragraphe 2 du présent article;

j) une description succincte de l'affaire.

([32]) Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (JO L 123 du 10.5.2019, p. 18).

6. Une injonction européenne de production est adressée au fournisseur de services agissant en qualité de responsable du traitement conformément au règlement (UE) 2016/679.

À titre exceptionnel, l'injonction européenne de production peut être adressée directement au fournisseur de services qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement, lorsque:

a) le responsable du traitement ne peut pas être identifié malgré des efforts raisonnables de la part de l'autorité d'émission; ou

b) le fait de s'adresser au responsable du traitement pourrait nuire à l'enquête.

7. Conformément au règlement (UE) 2016/679, le sous-traitant qui stocke ou traite d'une autre manière les données pour le compte du responsable du traitement informe celui-ci de la production des données, sauf si l'autorité d'émission a demandé au fournisseur de services de s'abstenir d'informer le responsable du traitement, aussi longtemps que cela est nécessaire et proportionné, afin de ne pas entraver la procédure pénale concernée. Dans ce cas, l'autorité d'émission indique dans le dossier les raisons du retard pris pour informer le responsable du traitement. Une brève justification est également ajoutée dans l'EPOC.

8. Lorsque les données sont stockées ou traitées d'une autre manière dans le cadre d'une infrastructure fournie par un fournisseur de services à une autorité publique, une injonction européenne de production ne peut être émise que si l'autorité publique pour laquelle les données sont stockées ou traitées d'une autre manière est située dans l'État d'émission.

9. Lorsque les données protégées par le secret professionnel en vertu du droit de l'État d'émission sont stockées ou traitées d'une autre manière par un fournisseur de services dans le cadre d'une infrastructure fournie à des professionnels soumis au secret professionnel («professionnel soumis au secret professionnel»), dans le cadre de leur activité professionnelle, une injonction européenne de production visant à obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou visant à obtenir des données relatives au contenu ne peut être émise que:

a) lorsque le professionnel soumis au secret professionnel réside dans l'État d'émission;

b) lorsque le fait de s'adresser à ce professionnel soumis au secret professionnel pourrait nuire à l'enquête; ou

c) lorsque le secret professionnel a été levé conformément au droit applicable.

10. Si l'autorité d'émission a des raisons de croire que les données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou les données relatives au contenu demandées par l'injonction européenne de production sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou que ces données sont soumises dans cet État à des règles relatives à la détermination et à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, l'autorité d'émission peut demander des éclaircissements avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État chargé de la mise en œuvre, soit directement, soit par l'intermédiaire d'Eurojust ou du réseau judiciaire européen.

L'autorité d'émission n'émet pas d'injonction européenne de production si elle constate que les données relatives au trafic demandées, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou que les données relatives au contenu sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou que ces données sont soumises dans cet État à des règles relatives à la détermination et à la limitation de la responsabilité pénale liées à la liberté de la presse et à la liberté d'expression dans d'autres médias.

Article 6

Conditions d'émission d'une injonction européenne de conservation

1. Une autorité d'émission ne peut émettre une injonction européenne de conservation que si les conditions énoncées au présent article sont remplies. L'article 5, paragraphe 8, s'applique mutatis mutandis.

2. Une injonction européenne de conservation doit être nécessaire et proportionnée aux fins d'empêcher le retrait, la suppression ou la modification de données en vue de l'émission d'une demande de production ultérieure 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 du suspect ou de la personne poursuivie.

3. Une injonction européenne de conservation peut être émise pour toutes les infractions pénales si elle aurait pu être émise dans les mêmes conditions dans le cadre d'une procédure nationale similaire, et pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté d'au moins quatre mois, prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

4. Une injonction européenne de conservation inclut les informations suivantes:

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

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

c) l'utilisateur, sauf si l'injonction a pour seule fin d'identifier l'utilisateur, ou tout autre identifiant unique tel que le nom d'utilisateur, l'identifiant de connexion ou le nom du compte afin de déterminer les données pour lesquelles la conservation est demandée;

d) la catégorie de données demandée telle qu'elle est définie à l'article 3, points 9) à 12);

e) s'il y a lieu, la période couverte par les données pour lesquelles la conservation est demandée;

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

g) les motifs qui permettent d'établir que l'injonction européenne de conservation remplit les conditions de nécessité et de proportionnalité visées au paragraphe 2 du présent article.

Article 7

Destinataires des injonctions européennes de production et des injonctions européennes de conservation

1. Les injonctions européennes de production et les injonctions européennes de conservation sont adressées directement à un établissement désigné ou à un représentant légal du fournisseur de services concerné.

2. À titre exceptionnel, dans les cas d'urgence tels qu'ils sont définis à l'article 3, point 18), lorsque l'établissement désigné ou le représentant légal d'un fournisseur de services ne réagit pas à un EPOC ou à un EPOC-PR dans les délais, cet EPOC ou cet EPOC-PR peut être adressé à tout autre établissement ou représentant légal du fournisseur de services dans l'Union.

Article 8

Notification à l'autorité chargée de la mise en œuvre

1. Lorsqu'une injonction européenne de production est émise afin d'obtenir des données relatives au trafic, à l'exception des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), ou afin d'obtenir des données relatives au contenu, l'autorité d'émission adresse une notification à l'autorité chargée de la mise en œuvre en lui transmettant l'EPOC qu'elle transmet dans le même temps au destinataire conformément à l'article 9, paragraphes 1 et 2.

2. Le paragraphe 1 ne s'applique pas si, lors de l'émission de l'injonction, l'autorité d'émission a des motifs raisonnables de croire que:

a) l'infraction a été commise, est en train d'être commise ou est susceptible d'être commise dans l'État d'émission; et

b) la personne dont les données sont demandées réside dans l'État d'émission.

3. Lorsqu'elle transmet l'EPOC comme cela est prévu au paragraphe 1 du présent article à l'autorité chargée de la mise en œuvre, l'autorité d'émission inclut, le cas échéant, toute information supplémentaire qui pourrait être nécessaire pour évaluer la possibilité d'invoquer un motif de refus conformément à l'article 12.

4. La notification à l'autorité chargée de la mise en œuvre visée au paragraphe 1 du présent article a un effet suspensif sur les obligations du destinataire énoncées à l'article 10, paragraphe 2, sauf dans les cas d'urgence tels qu'ils sont définis à l'article 3, point 18).

Article 9

Certificat d'injonction européenne de production (EPOC) et certificat d'injonction européenne de conservation (EPOC-PR)

1. Une injonction européenne de production ou une injonction européenne de conservation est transmise au destinataire tel qu'il est défini à l'article 7, au moyen d'un EPOC ou d'un EPOC-PR.

L'autorité d'émission ou, le cas échéant, l'autorité 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. Un EPOC contient les informations énumérées à l'article 5, paragraphe 5, points a) à h), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission et l'autorité chargée de la mise en œuvre, si nécessaire.

Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu de l'article 8, l'EPOC transmis à cette autorité contient les informations énumérées à l'article 5, paragraphe 5, points a) à j).

3. Un EPOC-PR contient les informations énumérées à l'article 6, paragraphe 4, points a) à f), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission.

4. Si nécessaire, l'EPOC ou l'EPOC-PR est traduit dans une langue officielle de l'Union acceptée par le destinataire, comme le prévoit l'article 4 de la directive (UE) 2023/1544. Si aucune langue n'a été spécifiée par le fournisseur de services, l'EPOC ou l'EPOC-PR est traduit dans une langue officielle de l'État membre où se trouve l'établissement désigné ou le représentant légal du fournisseur de services.

Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu de l'article 8, l'EPOC à transmettre à cette autorité est traduit dans une langue officielle de l'État chargé de la mise en œuvre ou dans une autre langue officielle de l'Union acceptée par cet État.

Article 10

Exécution d'un EPOC

1. Dès réception d'un EPOC, le destinataire agit rapidement pour conserver les données demandées.

2. Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu de l'article 8 et que cette autorité n'a invoqué aucun motif de refus conformément à l'article 12 dans les dix jours suivant la réception de l'EPOC, le destinataire veille à ce que les données demandées soient transmises directement à l'autorité d'émission ou aux autorités répressives, comme indiqué dans l'EPOC, à l'issue de cette période de dix jours. Lorsque l'autorité chargée de la mise en œuvre, avant même l'expiration du délai de dix jours, confirme à l'autorité d'émission et au destinataire qu'elle n'invoquera aucun motif de refus, le destinataire agit dès que possible après cette confirmation et au plus tard à l'expiration de ce délai de dix jours.

3. Lorsqu'une notification à l'autorité chargée de la mise en œuvre n'est pas requise en vertu de l'article 8, le destinataire veille, dès réception d'un EPOC, à ce que les données demandées soient transmises directement à l'autorité d'émission ou aux autorités répressives, comme indiqué dans l'EPOC, au plus tard dans un délai de dix jours suivant la réception de l'EPOC.

4. Dans les cas d'urgence, le destinataire transmet les données demandées sans retard injustifié, au plus tard dans les huit heures suivant la réception de l'EPOC. Lorsqu'une notification à l'autorité chargée de la mise en œuvre est requise en vertu de l'article 8, l'autorité chargée de la mise en œuvre peut, si elle décide d'invoquer un motif de refus conformément à l'article 12, paragraphe 1, notifier à l'autorité d'émission et au destinataire, sans retard et au plus tard dans les 96 heures suivant la réception de la notification, qu'elle s'oppose à l'utilisation des données ou que les données ne peuvent être utilisées que dans des conditions qu'elle précise. Lorsqu'un motif de refus est invoqué par l'autorité chargée de la mise en œuvre et que les données ont déjà été transmises par le destinataire à l'autorité d'émission, l'autorité d'émission efface les données ou autrement restreint l'utilisation des données ou, dans le cas où l'autorité chargée de la mise en œuvre a précisé des conditions, l'autorité d'émission respecte ces conditions lors de l'utilisation des données.

5. Lorsque le destinataire estime, sur la seule base des informations contenues dans l'EPOC, que l'exécution de l'EPOC pourrait interférer avec des immunités ou des privilèges, ou avec des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, en vertu du droit de l'État chargé de la mise en œuvre, le destinataire en informe l'autorité d'émission et l'autorité chargée de la mise en œuvre au moyen du formulaire figurant à l'annexe III.

Lorsqu'aucune notification à l'autorité chargée de la mise en œuvre n'a eu lieu en vertu de l'article 8, l'autorité d'émission tient compte des informations visées au premier alinéa du présent paragraphe et décide, de sa propre initiative ou à la demande de l'autorité chargée de la mise en œuvre, s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction européenne de production.

Lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu de l'article 8, l'autorité d'émission tient compte des informations visées au premier alinéa du présent paragraphe et décide s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction européenne de production. L'autorité chargée de la mise en œuvre peut décider d'invoquer les motifs de refus énoncés à l'article 12.

6. Lorsque le destinataire ne peut pas respecter son obligation de produire les données demandées parce que l'EPOC est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour être exécuté, il en informe, sans retard injustifié, l'autorité d'émission et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu de l'article 8, l'autorité chargée de la mise en œuvre visée dans l'EPOC, et demande des éclaircissements au moyen du formulaire figurant à l'annexe III. Dans le même temps, le destinataire indique à l'autorité d'émission si l'identification des données demandées et la conservation de ces données conformément au paragraphe 9 du présent article étaient possibles.

L'autorité d'émission réagit rapidement et au plus tard dans un délai de cinq jours suivant la réception du formulaire. Le destinataire s'assure qu'il peut recevoir les éclaircissements nécessaires ou toute correction apportée par l'autorité d'émission, afin de pouvoir remplir les obligations qui lui incombent énoncées aux paragraphes 1 à 4. Les obligations énoncées aux paragraphes 1 à 4 ne s'appliquent pas tant que l'autorité d'émission ou l'autorité chargée de la mise en œuvre n'a pas fourni de tels éclaircissements ou corrections.

7. Lorsque le destinataire ne peut pas respecter son obligation de produire les données demandées en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, il en informe, sans retard injustifié, l'autorité d'émission et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu de l'article 8, l'autorité chargée de la mise en œuvre visée dans l'EPOC, en expliquant les raisons de cette impossibilité de fait au moyen du formulaire figurant à l'annexe III. Lorsque l'autorité d'émission conclut à l'existence d'une telle impossibilité de fait, elle informe le destinataire et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu de l'article 8, l'autorité chargée de la mise en œuvre, qu'il n'est plus nécessaire d'exécuter l'EPOC.

8. Dans tous les cas où le destinataire ne fournit pas les données demandées, ne les fournit pas de manière exhaustive ou ne les fournit pas dans les délais impartis, pour des raisons autres que celles visées aux paragraphes 5, 6 et 7 du présent article, il informe de ces raisons, sans retard injustifié et au plus tard dans les délais énoncés aux paragraphes 2, 3 et 4 du présent article, l'autorité d'émission et, lorsqu'une notification à l'autorité chargée de la mise en œuvre a eu lieu en vertu de l'article 8, l'autorité chargée de la mise en œuvre visée dans l'EPOC, au moyen du formulaire figurant à l'annexe III. L'autorité d'émission réexamine l'injonction européenne de production à la lumière des informations fournies par le destinataire et, si nécessaire, fixe un nouveau délai pour que le destinataire produise les données.

9. Les données sont, dans la mesure du possible, conservées soit jusqu'à leur production, indépendamment du fait que cette production soit finalement demandée sur la base d'une injonction européenne de production clarifiée et de son EPOC ou par d'autres voies, telles que l'entraide judiciaire, soit jusqu'au retrait de l'injonction européenne de production.

Lorsque la production des données et leur conservation ne sont plus nécessaires, l'autorité d'émission et, s'il y a lieu en vertu de l'article 16, paragraphe 8, l'autorité chargée de la mise en œuvre informent le destinataire sans retard injustifié.

Article 11

Exécution d'un EPOC-PR

1. Dès réception d'un EPOC-PR, le destinataire conserve les données demandées, sans retard injustifié. L'obligation de conservation des données prend fin après soixante jours, à moins que l'autorité d'émission ne confirme, au moyen du formulaire figurant à l'annexe V, qu'une demande de production ultérieure a été émise. Au cours de cette période de soixante jours, l'autorité d'émission peut, au moyen du formulaire figurant à l'annexe VI, prolonger, si nécessaire, la durée de l'obligation de conservation des données d'une période supplémentaire de trente jours pour permettre l'émission d'une demande de production ultérieure.

2. Lorsque, au cours de la période de conservation visée au paragraphe 1, l'autorité d'émission confirme qu'une demande de production ultérieure a été émise, le destinataire conserve les données aussi longtemps que nécessaire pour produire les données une fois que la demande ultérieure aura été reçue.

3. Lorsque la conservation n'est plus nécessaire, l'autorité d'émission en informe sans retard injustifié le destinataire et l'obligation de conservation fondée sur l'injonction européenne de conservation concernée prend fin.

4. Lorsque le destinataire estime, sur la seule base des informations contenues dans l'EPOC-PR, que l'exécution de l'EPOC-PR pourrait interférer avec des immunités ou des privilèges, ou avec des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, en vertu du droit de l'État chargé de la mise en œuvre, il en informe l'autorité d'émission et l'autorité chargée de la mise en œuvre au moyen du formulaire figurant à l'annexe III.

L'autorité d'émission tient compte des informations visées au premier alinéa et décide, de sa propre initiative ou à la demande de l'autorité chargée de la mise en œuvre, s'il y a lieu de retirer, d'adapter ou de maintenir l'injonction européenne de conservation.

5. Lorsque le destinataire ne peut pas respecter son obligation de conserver les données demandées parce que l'EPOC-PR est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour être exécuté, il en informe, sans retard injustifié, l'autorité d'émission visée dans l'EPOC-PR et demande des éclaircissements au moyen du formulaire figurant à l'annexe III.

L'autorité d'émission réagit rapidement et au plus tard dans un délai de cinq jours à compter de la réception du formulaire. Le destinataire s'assure qu'il peut recevoir les éclaircissements nécessaires ou toute correction apportée par l'autorité d'émission, afin de pouvoir remplir les obligations qui lui incombent énoncées aux paragraphes 1, 2 et 3. En l'absence de réaction de l'autorité d'émission dans le délai de cinq jours, le fournisseur de services est exempté des obligations énoncées aux paragraphes 1 et 2.

6. Lorsque le destinataire ne peut pas respecter son obligation de conserver les données demandées en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, il en informe, sans retard injustifié, l'autorité d'émission visée dans l'EPOC-PR, en expliquant les raisons de cette impossibilité de fait au moyen du formulaire figurant à l'annexe III. Lorsque l'autorité d'émission conclut à l'existence d'une telle impossibilité, elle informe le destinataire qu'il n'est plus nécessaire d'exécuter l'EPOC-PR.

7. Dans tous les cas où le destinataire ne conserve pas les données demandées, pour des raisons autres que celles visées aux paragraphes 4, 5 et 6, il informe, sans retard injustifié, l'autorité d'émission de ces raisons au moyen du formulaire figurant à l'annexe III. L'autorité d'émission réexamine l'injonction européenne de conservation à la lumière de la justification fournie par le destinataire.

Article 12

Motifs de refus des injonctions européennes de production

1. Lorsque l'autorité d'émission a adressé une notification à l'autorité chargée de la mise en œuvre en vertu de l'article 8, et sans préjudice de l'article 1, paragraphe 3, l'autorité chargée de la mise en œuvre évalue les informations figurant dans l'injonction, dès que possible et au plus tard dans les dix jours suivant la réception de la notification ou, dans les cas d'urgence, au plus tard dans les 96 heures suivant la réception de la notification, et, le cas échéant, invoque un ou plusieurs des motifs de refus suivants:

a) les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre qui empêchent l'exécution ou la mise en œuvre de l'injonction, ou les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction;

b) dans des situations exceptionnelles, il existe des motifs sérieux de croire, sur la base d'éléments précis et objectifs, que l'exécution de l'injonction entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte;

c) l'exécution de l'injonction serait contraire au principe ne bis in idem;

d) les faits pour lesquels l'injonction a été émise ne constituent pas une infraction au titre du droit de l'État chargé de la mise en œuvre, à moins qu'ils ne concernent une infraction figurant dans les catégories d'infractions énumérées à l'annexe IV, 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 privatives de liberté d'une durée maximale d'au moins trois ans.

2. Lorsque l'autorité chargée de la mise en œuvre invoque un motif de refus en vertu du paragraphe 1, elle en informe le destinataire et l'autorité d'émission. Le destinataire met fin à l'exécution de l'injonction européenne de production et ne transfère pas les données, et l'autorité d'émission retire l'injonction.

3. Avant de décider d'invoquer un motif de refus, l'autorité chargée de la mise en œuvre à qui une notification a été adressée en vertu de l'article 8, prend contact avec l'autorité d'émission par tout moyen approprié afin d'examiner les mesures à prendre. Sur cette base, l'autorité d'émission peut décider d'adapter ou de retirer l'injonction européenne de production. Lorsque, à la suite de ces discussions, aucune solution n'est trouvée, l'autorité chargée de la mise en œuvre à qui une notification a été adressée en vertu de l'article 8 peut décider d'invoquer des motifs de refus de l'injonction européenne de production et en informe l'autorité d'émission et le destinataire en conséquence.

4. Lorsque l'autorité chargée de la mise en œuvre décide d'invoquer des motifs de refus en vertu du paragraphe 1, elle peut indiquer si elle s'oppose au transfert de toutes les données demandées dans l'injonction européenne de production ou si les données peuvent n'être que partiellement transférées ou utilisées dans les conditions fixées par l'autorité chargée de la mise en œuvre.

5. Lorsqu'une autorité de l'État chargé de la mise en œuvre a le pouvoir de lever l'immunité ou le privilège visés au paragraphe 1, point a), du présent article, l'autorité d'émission peut demander à l'autorité chargée de la mise en œuvre à qui une notification a été adressée en vertu de l'article 8 de prendre contact avec cette autorité de l'État chargé de la mise en œuvre afin de lui demander d'exercer ce pouvoir sans retard. Lorsque le pouvoir de lever l'immunité ou le privilège relève d'une autorité d'un autre État membre ou d'un pays tiers ou relève d'une organisation internationale, l'autorité d'émission peut demander à l'autorité concernée d'exercer ce pouvoir.

Article 13

Information de l'utilisateur et confidentialité

1. L'autorité d'émission informe, sans retard injustifié, la personne dont les données sont demandées au sujet de la production de données sur la base d'une injonction européenne de production.

2. L'autorité d'émission peut, conformément au droit national de l'État d'émission, retarder ou limiter l'information de la personne dont les données sont demandées, ou ne pas informer cette personne, dans la mesure où et aussi longtemps que les conditions de l'article 13, paragraphe 3, de la directive (UE) 2016/680 sont remplies, auquel cas l'autorité d'émission indique dans le dossier les raisons du retard ou de la limitation de l'information, ou de la non-information. Une brève justification est également ajoutée dans l'EPOC.

3. Lorsqu'elle informe la personne dont les données sont demandées conformément au paragraphe 1 du présent article, l'autorité d'émission fournit des informations sur les voies de recours disponibles en vertu de l'article 18.

4. Les destinataires et, s'il s'agit de personnes différentes, les fournisseurs de services prennent les mesures opérationnelles et techniques les plus modernes nécessaires 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.

Article 14

Remboursement des frais

1. Le fournisseur de services peut demander à l'État d'émission le remboursement de ses frais, si le droit national de l'État d'émission le prévoit pour les injonctions nationales dans des situations similaires, conformément au droit national de cet État. Les États membres informent la Commission de leurs règles nationales en matière de remboursement et la Commission les rend publiques.

2. Le présent article ne s'applique pas au remboursement des coûts du système informatique décentralisé visé à l'article 25.

CHAPITRE III

SANCTIONS ET MISE EN ŒUVRE

Article 15

Sanctions

1. Sans préjudice de leur droit national prévoyant d'imposer des sanctions pénales, les États membres déterminent le régime des sanctions pécuniaires applicables aux violations des articles 10 et 11 et de l'article 13, paragraphe 4, conformément à l'article 16, paragraphe 10, et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions pécuniaires prévues doivent être effectives, proportionnées et dissuasives. Les États membres veillent à ce que des sanctions pécuniaires allant jusqu'à 2 % du chiffre d'affaires annuel mondial total du fournisseur de services pour l'exercice précédent puissent être imposées. Les États membres informent la Commission, sans retard, du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.

2. Sans préjudice des obligations en matière de protection des données, les fournisseurs de services ne sont pas tenus responsables dans les États membres du préjudice causé à leurs utilisateurs ou à des tiers qui résulte exclusivement du respect de bonne foi d'un EPOC ou d'un EPOC-PR.

Article 16

Procédure de mise en œuvre

1. Lorsque le destinataire ne respecte pas un EPOC dans les délais impartis ou un EPOC-PR, sans fournir de raisons acceptées par l'autorité d'émission et, le cas échéant, lorsque l'autorité chargée de la mise en œuvre n'a invoqué aucun des motifs de refus énumérés à l'article 12, l'autorité d'émission peut demander à l'autorité chargée de la mise en œuvre de mettre en œuvre l'injonction européenne de production ou l'injonction européenne de conservation.

Aux fins de la mise en œuvre visée au premier alinéa, l'autorité d'émission transfère l'injonction concernée, le formulaire figurant à l'annexe III complété par le destinataire, et tout document pertinent conformément à l'article 19. L'autorité d'émission traduit l'injonction concernée, ainsi que tout document devant être transmis, dans l'une des langues acceptées par l'État chargé de la mise en œuvre et informe le destinataire du transfert.

2. Dès réception des documents, l'autorité chargée de la mise en œuvre reconnaît les injonctions ci-après, sans autres formalités, et prend les mesures nécessaires à leur mise en œuvre:

a) une injonction européenne de production, à moins qu'elle ne considère que l'un des motifs prévus au paragraphe 4 s'applique; ou

b) une injonction européenne de conservation, à moins qu'elle ne considère que l'un des motifs prévus au paragraphe 5 s'applique.

L'autorité chargée de la mise en œuvre décide de reconnaître ou non l'injonction sans retard injustifié et au plus tard dans un délai de cinq jours ouvrables suivant sa réception.

3. L'autorité chargée de la mise en œuvre enjoint formellement au destinataire de se conformer à ses obligations pertinentes et l'informe des éléments suivants:

a) la possibilité de formuler une objection à l'exécution de l'injonction concernée en invoquant un ou plusieurs des motifs énumérés au paragraphe 4, points a) à f), ou au paragraphe 5, points a) à e);

b) les sanctions applicables en cas de manquement; et

c) le délai de mise en conformité ou d'objection.

4. La mise en œuvre de l'injonction européenne de production ne peut être refusée que sur la base d'un ou de plusieurs des motifs suivants:

a) l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission prévue à l'article 4;

b) l'injonction européenne de production n'a pas été émise pour une infraction prévue à l'article 5, paragraphe 4;

c) le destinataire n'a pas pu se conformer à l'EPOC en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, ou parce que l'EPOC contient des erreurs manifestes;

d) l'injonction européenne de production ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'EPOC;

e) le service n'est pas couvert par le présent règlement;

f) les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction européenne de production;

g) dans des situations exceptionnelles, sur la base des seules informations contenues dans l'EPOC, il est évident qu'il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction européenne de production entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte.

5. La mise en œuvre de l'injonction européenne de conservation ne peut être refusée que sur la base d'un ou de plusieurs des motifs suivants:

a) l'injonction européenne de production n'a pas été émise ou validée par une autorité d'émission prévue à l'article 4;

b) le destinataire n'a pas pu se conformer à l'EPOC-PR en raison d'une impossibilité de fait due à des circonstances qui ne lui sont pas imputables, ou parce que l'EPOC-PR contient des erreurs manifestes;

c) l'injonction européenne de conservation ne concerne pas des données stockées par le fournisseur de services ou pour son compte au moment de la réception de l'EPOC-PR;

d) le service ne relève pas du champ d'application du présent règlement;

e) les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias, qui empêchent l'exécution ou la mise en œuvre de l'injonction européenne de conservation;

f) dans des situations exceptionnelles, sur la base des seules informations contenues dans l'EPOC-PR, il est évident qu'il existe des motifs sérieux de croire, sur la base d'éléments de preuve précis et objectifs, que l'exécution de l'injonction européenne de conservation entraînerait, dans les circonstances particulières de l'espèce, une violation manifeste d'un droit fondamental pertinent énoncé à l'article 6 du traité sur l'Union européenne et dans la Charte.

6. En cas d'objection du destinataire visée au paragraphe 3, point a), l'autorité chargée de la mise en œuvre décide de mettre en œuvre ou non l'injonction européenne de production ou l'injonction européenne de conservation sur la base de toute information fournie par le destinataire et, si nécessaire, des informations supplémentaires obtenues auprès de l'autorité d'émission conformément au paragraphe 7.

7. Avant de décider de ne pas reconnaître ou de ne pas mettre en œuvre l'injonction européenne de production ou l'injonction européenne de conservation conformément au paragraphe 2 ou 6 respectivement, l'autorité chargée de la mise en œuvre consulte l'autorité d'émission par tout moyen approprié. S'il y a lieu, elle demande des informations complémentaires à l'autorité d'émission. L'autorité d'émission répond à toute demande de ce type dans un délai de cinq jours ouvrables.

8. L'autorité chargée de la mise en œuvre notifie immédiatement toutes ses décisions à l'autorité d'émission et au destinataire.

9. Si l'autorité chargée de la mise en œuvre obtient du destinataire les données demandées par une injonction européenne de production, elle transmet ces données sans retard injustifié à l'autorité d'émission.

10. Lorsque le destinataire ne respecte pas les obligations qui lui incombent en vertu d'une injonction européenne de production ou d'une injonction européenne de conservation dont le caractère exécutoire a été confirmé par l'autorité chargée de la mise en œuvre, cette autorité impose une sanction pécuniaire conformément à l'article 15. Un recours juridictionnel effectif est disponible contre une décision d'imposer une sanction pécuniaire.

CHAPITRE IV

CONFLITS DE LOIS ET VOIES DE RECOURS

Article 17

Procédure de réexamen en cas d'obligations en conflit

1. Lorsqu'un destinataire considère que le respect d'une injonction européenne de production entrerait en conflit avec une obligation découlant du droit applicable d'un pays tiers, il informe l'autorité d'émission et l'autorité chargée de la mise en œuvre des raisons pour lesquelles il n'exécute pas l'injonction européenne de production, conformément à la procédure fixée à l'article 10, paragraphes 8 et 9, au moyen du formulaire figurant à l'annexe III («objection motivée»).

2. L'objection motivée comprend toutes les informations pertinentes sur le droit du pays tiers, son applicabilité en l'espèce et la nature de l'obligation en conflit. L'objection motivée n'est pas fondée sur:

a) le fait que des dispositions similaires concernant les conditions, les formalités et les procédures d'émission d'une injonction de production n'existent pas dans le droit applicable du pays tiers; ou

b) le seul fait que les données sont stockées dans un pays tiers.

L'objection motivée est formulée au plus tard dix jours après la date à laquelle le destinataire a reçu l'EPOC.

3. L'autorité d'émission réexamine l'injonction européenne de production sur la base de l'objection motivée et de toute contribution fournie par l'État chargé de la mise en œuvre. Lorsque l'autorité d'émission a l'intention de maintenir l'injonction européenne de production, elle demande un réexamen par la juridiction compétente de l'État d'émission. L'exécution de l'injonction européenne de production est suspendue en attendant la fin de la procédure de réexamen.

4. La juridiction compétente évalue d'abord s'il existe un conflit d'obligations, en examinant:

a) si le droit du pays tiers est applicable en fonction des circonstances spécifiques de l'affaire en question; et

b) si le droit du pays tiers, lorsqu'il est applicable conformément au point a), interdit la divulgation des données concernées lorsqu'il est appliqué aux circonstances particulières de l'affaire en question.

5. Lorsque la juridiction compétente constate qu'il n'existe pas de conflit d'obligations au sens des paragraphes 1 et 4, elle maintient l'injonction européenne de production.

6. Lorsque la juridiction compétente établit, sur la base de l'examen visé au paragraphe 4, point b), que le droit du pays tiers interdit la divulgation des données concernées, elle décide s'il y a lieu de maintenir ou de lever l'injonction européenne de production. Cette évaluation est en particulier fondée sur les facteurs suivants, une importance particulière étant accordée aux facteurs visés aux points a) et b):

a) l'intérêt protégé par la disposition de droit pertinente du pays tiers, y compris les droits fondamentaux ainsi que d'autres intérêts fondamentaux empêchant la divulgation des données, en particulier les intérêts liés à la sécurité nationale du pays tiers;

b) le degré de connexion entre l'affaire pénale pour laquelle l'injonction européenne de production a été émise et l'une ou l'autre des deux juridictions, comme l'indiquent entre autres:

   i) la localisation, la nationalité et le lieu de résidence de la personne dont les données sont demandées ou de la ou des victimes de l'infraction pénale en question;

   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; dans ce contexte, le lieu de stockage des données à lui seul ne suffit pas à établir un degré substantiel de connexion;

d) l'intérêt de l'État enquêteur à obtenir les preuves concernées, en fonction de la gravité de l'infraction et de l'importance d'obtenir rapidement des preuves;

e) les éventuelles conséquences pour le destinataire ou le fournisseur de services du respect de l'injonction européenne de production, y compris les éventuelles sanctions.

7. La juridiction compétente peut demander des informations auprès de l'autorité compétente du pays tiers, compte tenu de la directive (UE) 2016/680, en particulier de son chapitre V, et dans la mesure où cette demande n'entrave pas la procédure pénale concernée. L'État d'émission demande notamment des informations à l'autorité compétente du pays tiers lorsque le conflit d'obligations concerne des droits fondamentaux ou d'autres intérêts fondamentaux du pays tiers liés à la sécurité et à la défense nationales.

8. Si la juridiction compétente décide de lever l'injonction européenne de production, elle en informe l'autorité d'émission et le destinataire. Si la juridiction compétente décide que l'injonction européenne de production doit être maintenue, elle informe l'autorité d'émission et le destinataire, lequel procède à l'exécution de l'injonction.

9. Aux fins des procédures prévues par le présent article, les délais sont calculés conformément au droit national de l'autorité d'émission.

10. L'autorité d'émission informe l'autorité chargée de la mise en œuvre du résultat de la procédure de réexamen.

Article 18

Recours effectifs

1. Sans préjudice d'autres recours légaux disponibles conformément au droit national, toute personne dont les données ont été demandées au moyen d'une injonction européenne de production a droit à des recours effectifs contre cette injonction. Si cette personne est un suspect ou une personne poursuivie, elle a droit a des recours effectifs pendant la procédure pénale dans le cadre de laquelle les données ont été utilisées. Le droit à des recours effectifs visé au présent paragraphe est sans préjudice du droit de former un recours prévu par le règlement (UE) 2016/679 et la directive (UE) 2016/680.

2. Le droit à des recours effectifs s'exerce devant une juridiction de l'État d'émission conformément au droit de cet État et comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité, sans préjudice des garanties des droits fondamentaux dans l'État chargé de la mise en œuvre.

3. Aux fins de l'article 13, paragraphe 1, des informations sont fournies en temps utile sur les possibilités de former un recours prévues par le droit national et il est veillé à ce que ces recours puissent être effectivement exercés.

4. Les mêmes délais ou autres conditions pour la formation de recours dans le cadre de procédures nationales similaires s'appliquent aux fins du présent règlement et d'une manière qui garantit que les personnes concernées puissent exercer leur droit à ces recours de manière effective.

5. Sans préjudice des règles de procédure nationales, l'État d'émission et tout autre État membre auquel des preuves électroniques ont été transmises en vertu du présent règlement garantissent que les droits de la défense et l'équité de la procédure sont respectés lors de l'évaluation des preuves obtenues au moyen de l'injonction européenne de production.

CHAPITRE V

SYSTÈME INFORMATIQUE DÉCENTRALISÉ

Article 19

Communication numérique sécurisée et échange de données entre les autorités compétentes et les fournisseurs de services et entre les autorités compétentes

1. La communication écrite entre les autorités compétentes et les établissements désignés ou les représentants légaux au titre du présent règlement, y compris l'échange des formulaires prévus par le présent règlement et des données demandées dans le cadre d'une injonction européenne de production ou d'une injonction européenne de conservation, s'effectue au moyen d'un système informatique décentralisé sécurisé et fiable (ci-après dénommé «système informatique décentralisé»).

2. Chaque État membre veille à ce que les établissements désignés ou les représentants légaux des fournisseurs de services situés dans cet État membre aient accès au système informatique décentralisé par l'intermédiaire de leur système informatique national respectif.

3. Les fournisseurs de services veillent à ce que leurs établissements désignés ou leurs représentants légaux puissent utiliser le système informatique décentralisé via le système informatique national concerné afin de recevoir les EPOC et les EPOC-PR, d'envoyer les données demandées à l'autorité d'émission et de communiquer d'une autre manière avec l'autorité d'émission et l'autorité chargée de la mise en œuvre, comme le prévoit le présent règlement.

4. La communication écrite entre les autorités compétentes au titre du présent règlement, y compris l'échange des formulaires prévus par le présent règlement et des données demandées dans le cadre de la procédure de mise en œuvre prévue à l'article 16, ainsi que la communication écrite avec les agences ou organes compétents de l'Union, s'effectuent au moyen du système informatique décentralisé.

5. Lorsque la communication au moyen du système informatique décentralisé conformément au paragraphe 1 ou 4 n'est pas possible en raison, par exemple, d'une panne du système informatique décentralisé, de la nature des documents à transmettre, de contraintes techniques telles que le volume des données, de contraintes juridiques liées à la recevabilité des données demandées en tant que preuves ou aux exigences en matière de criminalistique applicables aux données demandées, ou de circonstances exceptionnelles, la transmission est effectuée à l'aide des moyens de substitution les plus appropriés, compte tenu de la nécessité de garantir la rapidité, la sécurité et la fiabilité de l'échange d'informations, et de permettre au destinataire d'en établir l'authenticité.

6. Lorsqu'une transmission est effectuée par des moyens de substitution comme le prévoit le paragraphe 5, l'autorité à l'origine de la transmission enregistre, sans retard injustifié, la transmission, y compris, s'il y a lieu, la date et l'heure de la transmission, l'expéditeur et le destinataire, le nom du fichier et sa taille, dans le système informatique décentralisé.

Article 20

Effets juridiques des documents électroniques

Les documents transmis dans le cadre d'une communication numérique ne sauraient être privés d'effet juridique et considérés comme irrecevables dans le cadre de procédures judiciaires transfrontières relevant du présent règlement au seul motif qu'ils se présentent sous forme numérique.

Article 21

Signatures et cachets électroniques

1. Le cadre juridique général régissant l'utilisation des services de confiance exposé dans le règlement (UE) n° 910/2014 s'applique aux communications électroniques relevant du présent règlement.

2. Lorsqu'un document transmis dans le cadre d'une communication numérique visée à l'article 19, paragraphe 1 ou 4, du présent règlement exige un cachet ou une signature conformément au présent règlement, il porte un cachet électronique qualifié ou une signature électronique qualifiée au sens du règlement (UE) n° 910/2014.

Article 22

Logiciel de mise en œuvre de référence

1. La Commission est responsable de la création, de la maintenance et du développement d'un logiciel de mise en œuvre de référence que les États membres peuvent choisir d'utiliser comme système dorsal en lieu et place d'un système informatique national. La création, la maintenance et le développement du logiciel de mise en œuvre de référence sont financés par le budget général de l'Union.

2. La Commission assure à titre gratuit la fourniture et la maintenance du logiciel de mise en œuvre de référence ainsi que l'assistance y afférente.

Article 23

Coûts du système informatique décentralisé

1. Chaque État membre prend en charge les coûts d'installation, d'exploitation et de maintenance des points d'accès du système informatique décentralisé relevant de sa responsabilité.

2. Chaque État membre prend en charge les coûts relatifs à l'établissement et à l'adaptation de ses systèmes informatiques nationaux nécessaires pour rendre ces systèmes interopérables avec les points d'accès, ainsi que les coûts de gestion, d'exploitation et de maintenance de ces systèmes.

3. Les agences et organes de l'Union prennent en charge les coûts d'installation, d'exploitation et de maintenance des composants du système informatique décentralisé relevant de leur responsabilité.

4. Les agences et organes de l'Union prennent en charge les coûts relatifs à l'établissement et à l'adaptation de leurs systèmes de gestion des dossiers nécessaires pour rendre ces systèmes interopérables avec les points d'accès, ainsi que les coûts de gestion, d'exploitation et de maintenance de ces systèmes.

5. Les fournisseurs de services prennent en charge tous les coûts nécessaires en vue d'intégrer le système informatique décentralisé ou d'interagir avec lui.

Article 24

Période de transition

Avant que l'obligation d'effectuer la communication écrite par l'intermédiaire du système informatique décentralisé visé à l'article 19 ne devienne applicable («période de transition»), la communication écrite entre les autorités compétentes et les établissements désignés ou les représentants légaux au titre du présent règlement s'effectue par les moyens de substitution les plus appropriés, compte tenu de la nécessité de garantir la rapidité, la sécurité et la fiabilité de l'échange d'informations. Lorsque les fournisseurs de services, les États membres ou les agences ou organes de l'Union ont mis en place des plateformes spécifiques ou d'autres canaux sécurisés pour le traitement des demandes de données par les autorités répressives et les autorités judiciaires, les autorités d'émission peuvent également choisir de transmettre un EPOC ou un EPOC-PR par ces canaux aux établissements désignés ou aux représentants légaux pendant la période de transition.

Article 25

Actes d'exécution

1. La Commission adopte les actes d'exécution nécessaires à l'établissement et à l'utilisation du système informatique décentralisé aux fins du présent règlement, lesquels précisent les éléments suivants:

a) les spécifications techniques définissant les méthodes de communication par voie électronique aux fins du système informatique décentralisé;

b) les spécifications techniques concernant les protocoles de communication;

c) les objectifs en matière de sécurité de l'information et les mesures techniques pertinentes garantissant des normes minimales de sécurité de l'information et un niveau élevé de cybersécurité pour le traitement et la communication des informations au sein du système informatique décentralisé;

d) les objectifs minimaux en matière de disponibilité et les éventuelles exigences techniques correspondantes pour les services fournis par le système informatique décentralisé;

2. Les actes d'exécution visés au paragraphe 1 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 26.

3. Les actes d'exécution visés au paragraphe 1 sont adoptés au plus tard le 18 août 2025.

Article 26

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

CHAPITRE VI

DISPOSITIONS FINALES

Article 27

Langues

Chaque État membre peut décider, à tout moment, d'accepter les traductions des EPOC et des EPOC-PR dans une ou plusieurs langues officielles de l'Union en plus de sa ou ses langues officielles, et communique cette décision à la Commission par déclaration écrite. La Commission met ces déclarations à la disposition de tous les États membres et du réseau judiciaire européen.

Article 28

Suivi et rapports

1. Au plus tard le 18 août 2026, la Commission établit un programme détaillé pour le suivi des réalisations, des résultats et des incidences du présent règlement. Le programme de suivi définit par quels moyens et dans quels intervalles les données seront collectées. Il précise quelles mesures la Commission et les États membres doivent prendre pour collecter et analyser les données.

2. En tout état de cause, à partir du 18 août 2026, les États membres collectent auprès des autorités compétentes des statistiques détaillées et les consignent. Les données collectées pour l'année civile précédente sont transmises à la Commission chaque année avant le 31 mars et comprennent:

a) le nombre d'EPOC et d'EPOC-PR émis, par type de données demandées, par destinataire et par situation (cas d'urgence ou non);

b) le nombre d'EPOC émis en vertu de dérogations pour les cas d'urgence;

c) le nombre d'EPOC et d'EPOC-PR honorés et non honorés, par type de données demandées, par destinataire et par situation (cas d'urgence ou non);

d) le nombre de notifications aux autorités chargées de la mise en œuvre qui ont eu lieu en vertu de l'article 8 et le nombre d'EPOC qui ont été refusés, par type de données demandées, par destinataire, par situation (cas d'urgence ou non) et par motif de refus invoqué;

e) pour les EPOC honorés, la durée moyenne entre le moment où l'EPOC a été émis et le moment où les données demandées ont été obtenues, par type de données demandées, par destinataire et par situation (cas d'urgence ou non);

f) pour les EPOC-PR honorés, la durée moyenne entre le moment où l'EPOC-PR a été émis et le moment où la demande de production ultérieure a été émise, par type de données demandées et par destinataire;

g) le nombre d'injonctions européennes de production et d'injonctions européennes de conservation transmises à un État chargé de la mise en œuvre et reçues par un tel État en vue de la mise en œuvre, par type de données requises, par destinataire et par situation (cas d'urgence ou non) ainsi que le nombre d'injonctions honorées;

h) le nombre de recours légaux formés contre les injonctions européennes de production dans l'État d'émission et dans l'État chargé de la mise en œuvre par type de données demandées;

i) le nombre de cas dans lesquels la validation ex post prévue à l'article 4, paragraphe 5, n'a pas été accordée;

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

3. À partir du 18 août 2026, en ce qui concerne les échanges de données effectués au moyen du système informatique décentralisé prévu à l'article 19, paragraphe 1, les statistiques visées au paragraphe 2 du présent article peuvent être collectées par les portails nationaux au moyen de programmes. Le logiciel de mise en œuvre de référence visé à l'article 22 est équipé techniquement pour assurer cette fonctionnalité.

4. Les fournisseurs de services peuvent collecter, consigner et publier des statistiques conformément aux principes existants en matière de protection des données. Si de telles statistiques sont collectées pour l'année civile précédente, elles peuvent être transmises à la Commission avant le 31 mars et peuvent comprendre, dans la mesure du possible:

a) le nombre d'EPOC et d'EPOC-PR reçus, par type de données demandées, par État d'émission et par situation (cas d'urgence ou non);

b) le nombre d'EPOC et EPOC-PR honorés et non honorés, par type de données demandées, par État d'émission et par situation (cas d'urgence ou non);

c) pour les EPOC honorés, la durée moyenne nécessaire à la fourniture des données demandées depuis le moment où l'EPOC a été reçu jusqu'au moment où les données ont été fournies, par type de données demandées, par État d'émission et par situation (cas d'urgence ou non);

d) pour les EPOC-PR honorés, la durée moyenne entre le moment où l'EPOC-PR a été émis et le moment où la demande de production ultérieure a été émise, par type de données demandées et par État d'émission.

5. À partir du 18 août 2027, la Commission publie, au plus tard le 30 juin de chaque année, un rapport contenant les données visées aux paragraphes 2 et 3, sous forme de compilation, comprenant une subdivision par État membre et par type de fournisseur de services.

Article 29

Modifications des certificats et des formulaires

La Commission adopte des actes délégués conformément à l'article 30 pour modifier les annexes I, II, III, V et VI afin de répondre efficacement à une éventuelle nécessité d'améliorer le contenu des formulaires EPOC et EPOC-PR et des formulaires à utiliser pour fournir des informations sur l'impossibilité d'exécuter un EPOC ou un EPOC-PR, pour confirmer l'émission d'une demande de production à la suite d'une injonction européenne de conservation et pour prolonger la conservation des preuves électroniques.

Article 30

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 29 est conféré à la Commission pour une durée indéterminée à compter du 18 août 2026.

3. La délégation de pouvoir visée à l'article 29 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 29 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 31

Notifications à la Commission

1. Au plus tard le 18 août 2025, chaque État membre adresse à la Commission des notifications portant sur ce qui suit:

a) l'autorité ou les autorités qui, conformément à son droit national, sont compétentes, conformément à l'article 4, pour émettre, valider ou transmettre des injonctions européennes de production et des injonctions européennes de conservation ou les notifications y afférentes;

b) l'autorité ou les autorités qui sont compétentes pour recevoir des notifications en vertu de l'article 8 et mettre en œuvre les injonctions européennes de production et les injonctions européennes de conservation pour le compte d'un autre État membre, conformément à l'article 16;

c) l'autorité ou les autorités qui sont compétentes pour traiter les objections motivées des destinataires conformément à l'article 17;

d) les langues acceptées pour la notification et la transmission d'un EPOC, d'un EPOC-PR, d'une injonction européenne de production ou d'une injonction européenne de conservation en cas de mise en œuvre, conformément à l'article 27.

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 Conseil ([33]).

Article 32

Rapport avec d'autres instruments, accords et arrangements

1. Le présent règlement ne porte pas atteinte aux instruments, conventions et accords de l'Union ou à d'autres instruments, conventions et accords internationaux relatifs à l'obtention de preuves qui relève du champ d'application du présent règlement.

2. Les États membres notifient à la Commission, au plus tard le 18 août 2026, les instruments, conventions et accords existants visés au paragraphe 1 qu'ils continueront d'appliquer. Les États membres notifient également à la Commission, dans les trois mois à compter de leur signature, toute nouvelle convention ou tout nouvel accord visé au paragraphe 1.

Article 33

Évaluation

Au plus tard le 18 août 2029, la Commission procède à une évaluation du présent règlement. Elle transmet un rapport d'évaluation au Parlement européen, au Conseil, au Contrôleur européen de la protection des données et à l'Agence des droits fondamentaux de l'Union européenne. Ce rapport d'évaluation comprend une évaluation de l'application du présent règlement et des résultats obtenus au regard de ses objectifs, ainsi qu'une évaluation de l'incidence du présent règlement sur les droits fondamentaux. 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 d'évaluation.

Article 34

Entrée en vigueur et application

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

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

2. Il est applicable à partir du 18 août 2026.

Toutefois, l'obligation faite aux autorités compétentes et aux fournisseurs de services d'utiliser le système informatique décentralisé établi à l'article 19 pour la communication écrite au titre du présent règlement s'applique à partir d'un an après l'adoption des actes d'exécution visés à l'article 25.

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

Fait à Strasbourg, le 12 juillet 2023.

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*
R. METSOLA	P. NAVARRO RÍOS

ANNEXE I

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

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil ([1]), le destinataire du présent certificat d'injonction européenne de production (EPOC) doit exécuter celui-ci et transmettre les données demandées, dans les délais visés à la section C du présent EPOC, à l'autorité compétente mentionnée à la section L, point a), du présent EPOC.

Dans tous les cas, le destinataire doit, à la réception de l'EPOC, agir rapidement pour conserver les données demandées, à moins que les informations contenues dans l'EPOC ne permettent pas d'identifier ces données. La conservation des données doit être 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 la mise en œuvre indique qu'il n'est plus nécessaire de conserver ni de produire les données.

Le destinataire doit prendre les mesures nécessaires pour garantir la confidentialité, le secret et l'intégrité de l'EPOC, ainsi que des données produites ou conservées.

SECTION A: Autorité d'émission/de validation

État d'émission: .....

Autorité d'émission: .....

Autorité de validation (le cas échéant): .....

NB: les coordonnées de l'autorité d'émission et de validation doivent être fournies à la fin du formulaire (sections I et J) .....

Numéro du dossier de l'autorité d'émission: .....

Numéro du dossier de l'autorité de validation: .....

SECTION B: Destinataire

Destinataire: .....

☐ Établissement désigné

☐ Représentant légal

☐ La présente injonction est émise dans un cas d'urgence à l'attention du destinataire indiqué parce que l'établissement désigné ou le représentant légal d'un fournisseur de services n'a pas réagi à l'EPOC dans les délais fixés à l'article 10 du règlement (UE) 2023/1543 ou n'a pas été désigné dans les délais fixés dans la directive (UE) 2023/1544 du Parlement européen et du Conseil ([2])

Adresse: .....

Téléphone/Télécopieur/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

([1]) Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation de preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

([2]) Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181).

SECTION C: Délais (cochez la case appropriée et complétez le cas échéant)

À la réception de l'EPOC, les données demandées doivent être produites:

☐ dès que possible et au plus tard dans un délai de dix jours (pas de notification à l'autorité chargée de la mise en œuvre);

☐ en cas de notification à l'autorité chargée de la mise en œuvre: à l'expiration du délai de dix jours, lorsque l'autorité chargée de la mise en œuvre n'a pas invoqué de motif de refus dans ce délai, ou lorsqu'elle confirme avant l'expiration du délai de dix jours qu'elle n'invoquera aucun motif de refus, dès que possible et au plus tard à la fin du délai de dix jours;

☐ sans retard injustifié et au plus tard dans un délai de huit heures dans un cas d'urgence impliquant:

☐ une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne;

☐ une menace imminente pour une infrastructure critique telle qu'elle est définie à l'article 2, point a), de la directive 2008/114/CE du Conseil ([3]) lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice des fonctions essentielles de l'État.

Précisez si des délais de procédure ou autres devraient être pris en compte pour l'exécution du présent EPOC: ....

Veuillez fournir des informations supplémentaires, s'il y a lieu: ....

SECTION D: Lien avec une demande de production ou de conservation antérieure (cochez et complétez le cas échéant et si ces informations sont disponibles)

☐ Les données demandées ont été totalement/partiellement conservées conformément à une demande de conservation

émise précédemment par ..... (indiquez l'autorité et le numéro de dossier)

le .... (indiquez la date d'émission de la demande)

et transmise le ..... (indiquez la date de transmission de la demande)

à ..... (indiquez le fournisseur de services/le représentant légal/l'établissement désigné/l'autorité compétente à qui la demande a été transmise et, s'il est disponible, le numéro de dossier attribué par le destinataire).

☐ Les données demandées sont liées à une demande de production

émise précédemment par ..... (indiquez l'autorité et le numéro de dossier)

le .... (indiquez la date d'émission de la demande)

et transmise le ..... (indiquez la date de transmission de la demande)

à ..... (indiquez le fournisseur de services/le représentant légal/l'établissement désigné/l'autorité compétente à qui la demande a été transmise et, s'il est disponible, le numéro de dossier attribué par le destinataire).

Autres informations utiles: ....

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

SECTION E: Informations à l'appui de l'identification des données demandées (complétez dans la mesure où ces informations sont connues et nécessaires pour identifier les données)

Adresse(s) IP et horodatages (y compris date et fuseau horaire): .....

Numéro de téléphone: ....

Adresse(s) électronique(s): ....

Numéro(s) IMEI: ....

Adresse(s) MAC: ....

Utilisateur(s) ou autre(s) identifiant(s) unique(s) tels que le ou les noms d'utilisateur, le ou les identifiants de connexion ou le ou les noms du compte: ....

Nom(s) du ou des services concernés: ....

Autre: ....

S'il y a lieu, la période couverte par les données pour lesquelles la production est demandée:

....

☐ Informations supplémentaires si nécessaire: ....

SECTION F: Preuves électroniques à produire

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

a) ☐ des données relatives aux abonnés:

☐ le nom, la date de naissance, l'adresse postale ou géographique 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 et des copies des documents fournis par l'abonné

☐ le type de service et sa durée, y compris le ou les identifiants utilisés par l'abonné ou qui lui a/ont été fourni(s) au moment du premier enregistrement ou de la première activation (par exemple numéro de téléphone, numéro de carte SIM, adresse MAC) et dispositif(s) associé(s)

☐ des informations relatives au profil (par exemple nom d'utilisateur, pseudonyme, 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 informations relatives à une carte de débit ou de crédit (fournies par l'utilisateur à des fins de facturation), y compris d'autres moyens de paiement

☐ des codes PUK

☐ autre: .....

b) ☐ des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543:

☐ les enregistrements des connexions IP, par exemple les adresses IP/journaux/numéros d'accès ainsi que tout autre identifiant technique, tel que les ports de provenance, l'horodatage ou équivalent, l'identifiant de l'utilisateur et l'interface utilisée dans le cadre de l'utilisation du service; veuillez préciser, si nécessaire: .....

☐ la période couverte par les données pour lesquelles la production est demandée (si elle est différente de la section E): ....

☐ autre: .....

c) ☐ les données relatives au trafic:

i) pour la téléphonie (mobile):

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

☐ l'heure et la durée de la ou des connexions

☐ la ou 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)

☐ autre: .....

ii) pour l'internet:

☐ les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur, informations de l'en-tête de courrier électronique, 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 ou des connexions

☐ le volume de données

☐ la date et l'heure de la ou des connexions

☐ la durée de la connexion ou de la ou des sessions d'accès

☐ autre: .....

iii) pour l'hébergement:

☐ les fichiers-journaux

☐ les tickets

☐ autre: .....

iv) autre:

☐ l'historique d'achats

☐ l'historique de rechargement du solde prépayé

☐ autre: .....

d) ☐ les données relatives au contenu:

☐ dump d'une boîte de messagerie (internet)

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

☐ dump de pages

☐ un journal/une sauvegarde de messages

☐ dump d'une messagerie vocale

☐ un contenu de serveurs

☐ une sauvegarde d'appareil

☐ une liste de contacts

☐ autre: .....

☐ Informations supplémentaires si nécessaire pour préciser ou limiter (davantage) l'éventail des données demandées: .....

SECTION G: Informations sur les conditions sous-jacentes

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

☐ une procédure pénale concernant une ou des infractions pénales;

☐ l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

b) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC est émis ainsi que la disposition légale applicable ([4]):

....

c) Le présent EPOC est délivré pour des données relatives au trafic qui ne sont pas demandées à la seule fin d'identifier l'utilisateur, ou pour des données relatives au contenu, ou les deux, et concerne (cochez la ou les cases appropriées, s'il y a lieu):

☐ 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;

([4]) Pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté en ce qui concerne des données relatives au trafic, qui ne sont pas demandées à la seule fin d'identifier l'utilisateur, ou des données relatives au contenu, veuillez indiquer aux points b) et c) l'infraction pour laquelle la peine a été imposée.

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

☐ une ou plusieurs des infractions définies aux articles 3 à 8 de la directive (UE) 2019/713 du Parlement européen et du Conseil ([5]);

☐ une ou plusieurs des infractions définies aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil ([6]);

☐ une ou plusieurs des infractions définies aux articles 3 à 8 de la directive 2013/40/UE du Parlement européen et du Conseil ([7]);

☐ des infractions pénales telles qu'elles sont définies aux articles 3 à 12 et à l'article 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil ([8]);

d) Responsable du traitement/sous-traitant:

Les injonctions européennes de production sont adressées aux fournisseurs de services agissant en qualité de responsables du traitement. À titre exceptionnel, l'injonction européenne de production peut être adressée directement au fournisseur de services qui traite les données pour le compte du responsable du traitement.

Cochez la ou les cases appropriées:

☐ Le présent EPOC est adressé au fournisseur de services agissant en qualité de responsable du traitement.

☐ Le présent EPOC est adressé au fournisseur de services qui traite ou, dans les situations où le responsable du traitement ne peut pas être identifié, qui pourrait traiter les données pour le compte du responsable du traitement, car:

☐ le responsable du traitement ne peut être identifié malgré des efforts raisonnables de la part de l'autorité d'émission;

☐ le fait de s'adresser au responsable du traitement pourrait nuire à l'enquête.

Si le présent EPOC est adressé au fournisseur de services traitant des données pour le compte du responsable du traitement:

☐ le sous-traitant informe le responsable du traitement de la production des données;

☐ le sous-traitant n'informe pas le responsable du traitement de la production des données jusqu'à nouvel ordre, car cela nuirait à l'enquête. Veuillez fournir une brève justification ([9]):

e) Autres informations utiles: ....

SECTION H: Informations à l'utilisateur

En tout état de cause, le destinataire s'abstient d'informer la personne dont les données sont demandées. Il incombe à l'autorité d'émission d'informer cette personne de la production des données, sans retard injustifié.

([5]) Directive (UE) 2019/713 du Parlement européen et du Conseil du 17 avril 2019 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil (JO L 123 du 10.5.2019, p. 18).

([6]) 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).

([7]) 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).

([8]) 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).

([9]) L'autorité d'émission doit indiquer les raisons du retard dans le dossier, seule une brève justification doit être ajoutée dans l'EPOC.

Veuillez noter que (cochez la ou les cases appropriées):

☐ l'autorité d'émission retardera l'information de la personne dont les données sont demandées, aussi longtemps qu'une ou plusieurs des conditions suivantes sont remplies:

☐ il est nécessaire d'éviter d'entraver des enquêtes, des recherches ou des procédures officielles ou judiciaires;

☐ il est nécessaire d'éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales;

☐ il est nécessaire de protéger la sécurité publique;

☐ il est nécessaire de protéger la sécurité nationale;

☐ il est nécessaire de protéger les droits et libertés de tiers.

SECTION I: Coordonnées de l'autorité d'émission

Type d'autorité d'émission (cochez la ou les cases appropriées):

☐ juge, juridiction ou juge d'instruction;

☐ procureur;

☐ autre autorité compétente déterminée par l'État d'émission.

Si une validation est nécessaire, veuillez également compléter la section J.

Veuillez noter que (cochez le cas échéant):

☐ Le présent EPOC a été émis pour des données relatives aux abonnés, ou pour des données demandées à la seule fin d'identifier l'utilisateur, dans un cas d'urgence dont l'existence est établie de manière valable sans validation préalable, parce que la validation n'aurait pas pu être obtenue à temps, ou pour les deux catégories de données. L'autorité d'émission confirme qu'elle pourrait émettre une injonction sans validation dans le cadre d'une procédure nationale similaire, et qu'elle demandera la validation ex post sans retard injustifié, au plus tard dans les 48 heures (veuillez noter que le destinataire ne sera pas informé).

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

Nom de l'autorité: .....

Nom de son représentant: .....

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

Numéro de dossier: .....

Adresse: .....

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

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

Adresse électronique: .....

Langue(s) parlée(s): ....

Si elle ou il diffère de ceux indiqués précédemment, autorité/point de contact (par exemple l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC:

Nom de l'autorité/nom: ....

Adresse: ....

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

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

Adresse électronique: ....

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

Date: ....

Signature ([10]):

SECTION J: Coordonnées de l'autorité de validation (complétez le cas échéant)

Type d'autorité de validation

☐ juge, juridiction ou juge d'instruction

☐ procureur

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

Nom de l'autorité: ....

Nom de son représentant: ....

Fonction (titre/grade): ....

Numéro de dossier: ....

Adresse: ....

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

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

Adresse électronique: ....

Langue(s) parlée(s): ....

([10]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

Date: ....

Signature ([11]):

SECTION K: Notification et coordonnées de l'autorité chargée de la mise en œuvre à qui une notification est adressée (le cas échéant)

☐ Le présent EPOC est notifié à l'autorité chargée de la mise en œuvre suivante:.....

Veuillez indiquer les coordonnées de l'autorité chargée de la mise en œuvre à qui une notification est adressée (si elles sont disponibles):

Nom de l'autorité chargée de la mise en œuvre: ....

Adresse: ....

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

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

Adresse électronique: ....

SECTION L: Transfert de données

a) Autorité à qui les données doivent être transférées

☐ autorité d'émission

☐ autorité de validation

☐ autre autorité compétente (par exemple autorité centrale)

Nom et coordonnées de contact: ....

b) Format privilégié dans lequel les données doivent être transférées ou moyen de transfert privilégié (le cas échéant): ....

SECTION M: Informations complémentaires à inclure (à ne pas envoyer au destinataire — à fournir à l'autorité chargée de la mise en œuvre dans le cas où la notification à l'autorité chargée de la mise en œuvre est requise)

Motifs qui permettent d'établir que l'injonction européenne de conservation remplit les conditions de la nécessité et de la proportionnalité:

....

Description succincte de l'affaire:

....

([11]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

L'infraction pour laquelle l'injonction européenne de production est émise est-elle passible dans l'État d'émission d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans et figure-t-elle dans la liste d'infractions ci-dessous (cochez la ou les cases appropriées)?

☐ 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 et les autres infractions pénales portant atteinte aux intérêts financiers de l'Union définies dans la directive (UE) 2017/1371 du Parlement européen et du Conseil ([12]);

☐ 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;

☐ homicide volontaire ou coups et blessures graves;

☐ trafic d'organes et de tissus humains;

☐ enlèvement, séquestration ou prise d'otage;

☐ racisme et xénophobie;

☐ vol organisé ou 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;

([12]) Directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO L 198 du 28.7.2017, p. 29).

☐ 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'aéronefs ou de navires;

☐ sabotage.

Le cas échéant, veuillez ajouter toute information supplémentaire dont l'autorité chargée de la mise en œuvre pourrait avoir besoin pour évaluer la possibilité d'invoquer des motifs de refus:

… ....

ANNEXE II

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

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire du présent certificat d'injonction européenne de conservation (EPOC-PR) doit, sans retard injustifié après réception de l'EPOC-PR, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne prolonge ce délai de 30 jours supplémentaires ou ne confirme qu'une demande de production ultérieure a été émise. Si l'autorité d'émission confirme dans ces délais qu'une demande de production ultérieure a été émise, le destinataire doit conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande de production ultérieure aura été reçue.

Le destinataire doit prendre les mesures nécessaires pour garantir la confidentialité, le secret et l'intégrité de l'EPOC-PR, ainsi que des données conservées.

SECTION A: Autorité d'émission/de validation

État d'émission: ....

Autorité d'émission: ....

Autorité de validation (le cas échéant): ....

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

Numéro du dossier de l'autorité d'émission: ....

Numéro du dossier de l'autorité de validation: ....

SECTION B: Destinataire

Destinataire: ....

☐ Établissement désigné

☐ Représentant légal

☐ La présente injonction est émise dans un cas d'urgence à l'attention du destinataire indiqué parce que l'établissement désigné ou le représentant légal d'un fournisseur de services n'a pas réagi à l'EPOC-PR dans les délais ou n'a pas été désigné dans les délais fixés dans la directive (UE) 2023/1544 du Parlement européen et du Conseil [2]

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

[2] Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181).

Adresse: .....

Téléphone/Télécopie/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

SECTION C: Informations à l'appui de l'identification des données dont la conservation a été demandée (complétez dans la mesure où ces informations sont connues et nécessaires pour identifier les données)

☐ Adresse(s) IP et horodatages (y compris date et fuseau horaire): .....

☐ Numéro de téléphone: .....

☐ Adresse(s) électronique(s): .....

☐ Numéro(s) IMEI: .....

☐ Adresse(s) MAC: .....

☐ Utilisateur(s) du service ou autre(s) identifiant(s) unique(s) tels que le ou les noms d'utilisateur, le ou les identifiants de connexion ou le ou les noms du compte .....

☐ Nom(s) du ou des services concernés: .....

☐ Autres informations: .....

S'il y a lieu, la période couverte par les données pour lesquelles la conservation est demandée: .....

☐ Informations supplémentaires si nécessaire: .....

SECTION D: Preuves électroniques à conserver

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

a) ☐ des données relatives aux abonnés:

☐ le nom, la date de naissance, l'adresse postale ou géographique 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 et sa durée, y compris le ou les identifiants utilisés par l'abonné ou qui lui a/ont été fourni (s) au moment du premier enregistrement ou de la première activation (par exemple numéro de téléphone, numéro de carte SIM, adresse MAC) et dispositif(s) associé(s)

☐ des informations relatives au profil (par exemple nom d'utilisateur, pseudonyme, 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 informations relatives à une carte de débit ou de crédit (fournies par l'utilisateur à des fins de facturation), y compris d'autres moyens de paiement

☐ des codes PUK

☐ autre: ....

b) ☐ des données demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543:

☐ les enregistrements des connexions IP, par exemple les adresses IP/journaux/numéros d'accès ainsi que tout autre identifiant, tel que les ports de provenance, l'horodatage ou équivalent, l'identifiant de l'utilisateur et l'interface utilisée dans le cadre de l'utilisation du service, strictement nécessaire à des fins d'identification; veuillez préciser, si nécessaire: ....

☐ la période couverte par les données pour lesquelles la conservation est demandée (si elle est différente de la section C):..... .....

☐ autre: ....

c) ☐ les données relatives au trafic;

i) pour la téléphonie (mobile):

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

☐ l'heure et la durée de la ou des connexions

☐ la ou 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)

☐ autre: ....

ii) pour l'internet:

☐ les informations d'acheminement [adresse IP d'origine, adresse(s) IP de destination, numéro(s) de port, navigateur, informations de l'en-tête de courrier électronique, 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 ou des connexions

☐ le volume de données

☐ la date et l'heure de la ou des connexions

☐ la durée de la connexion ou de la ou des sessions d'accès

☐ autre: ....

iii) pour l'hébergement:

☐ les fichiers-journaux

☐ les tickets

☐ autre: ....

iv) autre

☐ l'historique d'achats

☐ l'historique de rechargement du solde prépayé

☐ autre: ....

d) ☐ des données relatives au contenu:

☐ dump d'une boîte de messagerie (internet)

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

☐ dump de pages

☐ un journal/une sauvegarde de messages

☐ dump d'une messagerie vocale

☐ un contenu de serveurs

☐ une sauvegarde d'appareil

☐ une liste de contacts

☐ autre: ....

☐ Informations supplémentaires si nécessaire pour préciser ou limiter (davantage) la période couverte par les données demandées:..... .....

SECTION E: Informations sur les conditions sous-jacentes

a) Le présent EPOC-PR concerne (cochez la ou les cases appropriées):

☐ une procédure pénale concernant une infraction pénale;

☐ l'exécution d'une peine ou mesure de sûreté privatives de liberté d'une durée d'au moins quatre mois prononcées, à l'issue d'une procédure pénale, par une décision qui n'a pas été rendue par défaut, dans les cas où la personne condamnée s'est soustraite à la justice.

b) Nature et qualification juridique de l'infraction ou des infractions pour lesquelles l'EPOC-PR est émis ainsi que la disposition légale applicable ([3]):..... .....

SECTION F: Coordonnées de l'autorité d'émission

Type d'autorité d'émission (cochez la ou les cases appropriées):

☐ juge, juridiction ou juge d'instruction;

☐ procureur;

☐ autre autorité compétente telle qu'elle est déterminée par le droit de l'État d'émission.

Si une validation est nécessaire, veuillez également compléter la section G.

Veuillez noter que (cochez le cas échéant):

☐ Le présent EPOC-PR a été émis pour des données relatives aux abonnés, ou pour des données demandées à la seule fin d'identifier l'utilisateur, dans un cas d'urgence dont l'existence est établie de manière valable, sans validation préalable, parce que la validation n'aurait pas pu être obtenue à temps, ou pour les deux catégories de données. L'autorité d'émission confirme qu'elle pourrait émettre une injonction sans validation dans le cadre d'une procédure nationale similaire et qu'elle demandera la validation ex post sans retard injustifié, au plus tard dans les 48 heures (veuillez noter que le destinataire ne sera pas informé).

Ce cas d'urgence renvoie à une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, ou une menace imminente pour une infrastructure critique, telle qu'elle est définie à l'article 2, point a), de la directive 2008/114/CE du Conseil ([4]), lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie, l'intégrité physique ou la sécurité d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice des fonctions essentielles de l'État.

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):..... .....

([3]) Pour l'exécution d'une peine ou d'une mesure de sûreté privatives de liberté, veuillez indiquer l'infraction pour laquelle la peine a été imposée.

([4]) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes (JO L 345 du 23.12.2008, p. 75).

Numéro de dossier: .....

Adresse: .....

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

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

Adresse électronique: .....

Langue(s) parlée(s): .....

Si elle ou il diffère de ceux indiqués précédemment, autorité/point de contact (par exemple l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom de l'autorité/nom: .....

Adresse: .....

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

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

Adresse électronique: .....

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

Date: .....

Signature ([5]): .....

SECTION G: Coordonnées de l'autorité de validation (complétez le cas échéant)

Type d'autorité de validation:

☐ juge, juridiction ou juge d'instruction

☐ procureur

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

Nom de l'autorité: .....

Nom de son représentant: .....

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

([5]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

Numéro de dossier: .....

Adresse: .....

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

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

Adresse électronique: .....

Langue(s) parlée(s): .....

Date: .....

Signature ([6]): .....

([6]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE III

INFORMATIONS CONCERNANT L'IMPOSSIBILITÉ D'EXÉCUTER UN EPOC/EPOC-PR

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], lorsque le destinataire n'est pas en mesure de respecter son obligation de conserver les données demandées en vertu d'un EPOC-PR ou de les produire en vertu d'un EPOC, n'est pas en mesure de respecter le délai spécifié ou ne fournit pas les données de manière exhaustive, il convient que le destinataire remplisse le présent formulaire et le renvoie, sans retard injustifié, à l'autorité d'émission ainsi que, si une notification a eu lieu et dans les autres cas où cela s'impose, à l'autorité chargée de la mise en œuvre visée dans l'EPOC.

Dans la mesure du possible, le destinataire conserve les données requises, même lorsque des informations supplémentaires sont nécessaires pour identifier les données de manière précise, sauf si les informations qui figurent dans l'EPOC/EPOC-PR ne sont pas suffisantes à cet effet. Si des éclaircissements de la part de l'autorité d'émission sont nécessaires, le destinataire les demande, sans retard injustifié, au moyen du présent formulaire.

SECTION A: Certificat concerné

Les informations suivantes concernent:

☐ un certificat d'injonction européenne de production (EPOC)

☐ un certificat d'injonction européenne de conservation (EPOC-PR)

SECTION B: Autorité ou autorités concernées

Autorité d'émission:.....

Numéro du dossier de l'autorité d'émission:.....

Le cas échéant, autorité de validation:.....

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

Date d'émission de l'EPOC/EPOC-PR:.....

Date de réception de l'EPOC/EPOC-PR:.....

Le cas échéant, autorité chargée de la mise en œuvre:.....

Numéro du dossier de l'autorité chargée de la mise en œuvre, s'il est disponible:.....

SECTION C: Destinataire de l'EPOC/EPOC-PR

Destinataire de l'EPOC/EPOC-PR:.....

Numéro du dossier du destinataire:.....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION D: Raisons de la non-exécution

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

☐ il est incomplet;

☐ il contient des erreurs manifestes;

☐ il ne contient pas suffisamment d'informations;

☐ il ne concerne pas des données stockées par le fournisseur de services ou pour le compte de celui-ci au moment de la réception de l'EPOC/EPOC-PR;

☐ autres motifs d'impossibilité de fait due à des circonstances qui ne sont pas imputables au destinataire ou au fournisseur de services au moment de la réception de l'EPOC/EPOC-PR;

☐ l'injonction européenne de production/l'injonction européenne de conservation n'a pas été émise ou validée par une autorité d'émission mentionnée à l'article 4 du règlement (UE) 2023/1543;

☐ l'injonction européenne de production visant à obtenir des données relatives au trafic qui ne sont pas demandées à la seule fin d'identifier l'utilisateur telles qu'elles sont définies à l'article 3, point 10), du règlement (UE) 2023/1543, ou visant à obtenir des données relatives au contenu, a été émise pour une infraction qui n'est pas visée à l'article 5, paragraphe 4, du règlement (UE) 2023/1543;

☐ le service n'est pas couvert par le règlement (UE) 2023/1543;

☐ les données demandées sont protégées par des immunités ou des privilèges accordés en vertu du droit de l'État chargé de la mise en œuvre, ou les données demandées sont couvertes par des règles relatives à la détermination ou à la limitation de la responsabilité pénale liées à la liberté de la presse ou à la liberté d'expression dans d'autres médias qui empêchent l'exécution de l'injonction européenne de production ou de l'injonction européenne de conservation;

☐ le respect de l'injonction européenne de production entrerait en conflit avec le droit applicable d'un pays tiers. Veuillez également compléter la section E.

b) Veuillez préciser les raisons de la non-exécution visée au point a) et, si nécessaire, indiquez et expliquez toute raison autre que celles énumérées au point a):

… ....

SECTION E: Obligations en conflit découlant du droit d'un pays tiers

En cas d'obligations en conflit découlant du droit d'un pays tiers, veuillez fournir les informations suivantes:

— intitulé du ou des actes juridiques du pays tiers:

… ....

— disposition(s) légale(s) applicable(s) et texte de la ou des dispositions pertinentes:

… ....

— nature de l'obligation en conflit, y compris l'intérêt protégé par le droit 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 le droit 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:

… ....

Veuillez ajouter toute information supplémentaire pertinente: ....

SECTION F: Demande d'informations supplémentaires/d'éclaircissements (veuillez compléter le cas échéant)

Des informations supplémentaires sont requises de la part de l'autorité d'émission afin que l'EPOC/EPOC-PR soit exécuté:

… ....

SECTION G: Conservation des données

Les données demandées (cochez la case appropriée et complétez):

☐ ont été conservées 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 la mise en œuvre, indique qu'il n'est plus nécessaire de conserver ni de produire les données, ou jusqu'à ce que l'autorité d'émission fournisse les informations nécessaires pour permettre de circonscrire les données à conserver/produire;

☐ n'ont pas été conservées (cela ne devrait s'appliquer qu'à titre exceptionnel, par exemple si le fournisseur de services ne détient pas les données à la réception de la demande ou ne peut pas suffisamment identifier les données demandées).

SECTION H: Coordonnées de l'établissement désigné/du représentant légal du fournisseur de services

Nom de l'établissement désigné/du représentant légal du fournisseur de services:
.....

Nom du point de contact: ....

Poste occupé: .....

Adresse: .....

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

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

Adresse électronique: .....

Nom de la personne autorisée: ....

Date: .....

Signature ([2]): .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE IV

CATÉGORIES D'INFRACTIONS VISÉES À L'ARTICLE 12, PARAGRAPHE 1, POINT D)

1) participation à une organisation criminelle;

2) terrorisme;

3) traite des êtres humains;

4) exploitation sexuelle des enfants et pédopornographie;

5) trafic de stupéfiants et de substances psychotropes;

6) trafic d'armes, de munitions et d'explosifs;

7) corruption;

8) fraude, y compris la fraude et les autres infractions pénales portant atteinte aux intérêts financiers de l'Union définies dans la directive (UE) 2017/1371 du Parlement européen et du Conseil ([1]);

9) blanchiment des produits du crime;

10) faux monnayage et contrefaçon de monnaie, y compris de l'euro;

11) cybercriminalité;

12) crimes contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées;

13) aide à l'entrée et au séjour irréguliers;

14) homicide volontaire ou coups et blessures graves;

15) trafic d'organes et de tissus humains;

16) enlèvement, séquestration ou prise d'otage;

17) racisme et xénophobie;

18) vol organisé ou à main armée;

19) trafic de biens culturels, y compris d'antiquités et d'œuvres d'art;

20) escroquerie;

21) racket et extorsion de fonds;

22) contrefaçon et piratage de produits;

([1]) Directive (UE) 2017/1371 du Parlement européen et du Conseil du 5 juillet 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal (JO L 198 du 28.7.2017, p. 29).

23) falsification de documents administratifs et trafic de faux;

24) falsification de moyens de paiement;

25) trafic de substances hormonales et d'autres facteurs de croissance;

26) trafic de matières nucléaires et radioactives;

27) trafic de véhicules volés;

28) viol;

29) incendie volontaire;

30) crimes relevant de la compétence de la Cour pénale internationale;

31) détournement d'aéronefs ou de navires;

32) sabotage.

ANNEXE V

CONFIRMATION DE L'ÉMISSION D'UNE DEMANDE DE PRODUCTION À LA SUITE D'UNE INJONCTION EUROPÉENNE DE CONSERVATION

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire de l'EPOC-PR doit, après réception et sans retard injustifié, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne prolonge ce délai de 30 jours supplémentaires ou ne confirme qu'une demande de production ultérieure a été émise au moyen du formulaire figurant dans la présente annexe.

À la suite de cette confirmation, le destinataire doit conserver les données aussi longtemps que nécessaire pour pouvoir produire les données une fois que la demande de production ultérieure aura été reçue.

SECTION A: Autorité d'émission de l'EPOC-PR

État d'émission: .....

Autorité d'émission: .....

Si elle ou il diffère du point de contact indiqué dans l'EPOC-PR, autorité/point de contact (par exemple, l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom et coordonnées de contact: .....

SECTION B: Destinataire de l'EPOC-PR

Destinataire: .....

Adresse: .....

Téléphone/télécopie/adresse électronique (s'ils sont connus): .....

Personne de contact (si elle est connue): .....

Numéro du dossier du destinataire (s'il est connu): .....

Fournisseur de services concerné (s'il est différent du destinataire): .....

Autres informations utiles: .....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION C: Informations sur l'EPOC-PR

Les données sont conservées conformément à l'EPOC-PR émis le..... (indiquez la date d'émission de la demande) et transmis le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier).

☐ Le délai a été prolongé de 30 jours par l'autorité d'émission …, numéro de dossier … le … (veuillez cocher la case et compléter, le cas échéant).

SECTION D: Confirmation

Le présent document confirme que la demande de production suivante a été émise (veuillez cocher la case appropriée et compléter, le cas échéant):

☐ Certificat d'injonction européenne de production émis par ..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmis le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmis à..... (indiquez le fournisseur de services/l'établissement désigné/le représentant légal/l'autorité compétente à qui il a été transmis et, s'il est disponible, le numéro de dossier attribué par le destinataire).

☐ Décision d'enquête européenne émise par..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmise le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmise à..... (indiquez l'État et l'autorité compétente à qui elle a été transmise et, s'il est disponible, le numéro de dossier attribué par les autorités requises).

☐ Demande d'entraide judiciaire émise par ..... (indiquez l'autorité) le..... (indiquez la date d'émission de la demande) et transmise le..... (indiquez la date de transmission de la demande) avec le numéro de dossier ..... (indiquez le numéro de dossier) et transmise à..... (indiquez l'État et l'autorité compétente à qui elle a été transmise et, s'il est disponible, le numéro de dossier attribué par les autorités requises).

Signature de l'autorité d'émission et/ou de son représentant:

Nom: .....

Date: .....

Signature ([2]): .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.

ANNEXE VI

PROLONGATION DE LA CONSERVATION DE PREUVES ÉLECTRONIQUES

Conformément au règlement (UE) 2023/1543 du Parlement européen et du Conseil [1], le destinataire du certificat d'injonction européenne de conservation (EPOC-PR) doit, après réception et sans retard injustifié, conserver les données demandées. La conservation doit prendre fin après 60 jours, à moins que l'autorité d'émission ne confirme que la demande de production ultérieure a été émise. Dans le délai de 60 jours, l'autorité d'émission peut prolonger la durée de conservation de 30 jours supplémentaires, le cas échéant, pour permettre que la demande de production ultérieure soit émise, au moyen du formulaire figurant dans la présente annexe.

SECTION A: Autorité d'émission de l'EPOC-PR

État d'émission: … ....

Autorité d'émission: … .....

Numéro du dossier de l'autorité d'émission: …..... .

Si elle ou il diffère du point de contact indiqué dans l'EPOC-PR, autorité/point de contact (par exemple, l'autorité centrale) à contacter pour toute question liée à l'exécution de l'EPOC-PR:

Nom et coordonnées de contact: …..... .....

SECTION B: Destinataire de l'EPOC-PR

Destinataire: …..... .....

Adresse: … ....

Téléphone/télécopieur/adresse électronique (s'ils sont connus): …..... .....

Personne de contact (si elle est connue): …..... .....

Numéro du dossier du destinataire (s'il est connu): … .....

Fournisseur de services concerné (s'il est différent du destinataire): …..... .....

Autres informations utiles: …..... .....

SECTION C: Informations sur l'EPOC-PR préalable

Les données sont conservées conformément à l'EPOC-PR émis le …..... (indiquez la date d'émission de la demande) et transmis le … ..... (indiquez la date de transmission de la demande) avec le numéro de dossier …..... (indiquez le numéro de dossier) et transmis à …..... .....

[1] Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale (JO L 191 du 28.7.2023, p. 118).

SECTION D: Prolongation de l'injonction de conservation préalable

L'obligation de conserver les données au titre de l'EPOC-PR visé à la section C est prolongée par la présente de trente jours supplémentaires.

Signature de l'autorité d'émission et/ou de son représentant:

Nom: … .....

Date: … .....

Signature ([2]): … .....

([2]) Si le système informatique décentralisé n'est pas utilisé, veuillez également ajouter un cachet officiel, un cachet électronique ou une authentification équivalente.