Conseil de
l'Union européenne

Bruxelles, le 18 avril 2018
(OR. en)

8110/18

Dossier interinstitutionnel:
2018/0108 (COD)

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PROPOSITION

Origine:	Pour le secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, directeur
Date de réception:	18 avril 2018
Destinataire:	Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2018) 225 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

Les délégations trouveront ci-joint le document COM(2018) 225 final.

p.j.: COM(2018) 225 final

COMMISSION
EUROPÉENNE

Strasbourg, le 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

{SEC(2018) 199 final} - {SWD(2018) 118 final} - {SWD(2018) 119 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

De nos jours, il est devenu banal, dans une grande partie du monde, d'utiliser les médias sociaux, les messageries web et les services et applications de messagerie pour communiquer, travailler, socialiser et obtenir des informations. Ces services permettent à des centaines de millions d'utilisateurs de se connecter entre eux. Ils contribuent considérablement au bien-être économique et social des utilisateurs au sein de l'Union et à l'extérieur. Cependant, ils peuvent aussi être utilisés à mauvais escient pour commettre ou faciliter des actes criminels, y compris des crimes graves tels que des attaques terroristes. Lorsque cela se produit, ces services et applications constituent souvent la seule source d'indices permettant aux enquêteurs d'identifier l'auteur d'un crime et d'obtenir des preuves qui pourront être utilisées devant les juridictions.

Étant donné la nature transfrontière de l'internet, il est possible de fournir ces services depuis n'importe quel endroit dans le monde, sans avoir nécessairement besoin d'infrastructure physique, d'entreprise ni de personnel dans les États membres où ils sont proposés ou sur le marché intérieur dans son ensemble. Ils ne requièrent pas non plus de lieu spécifique pour le stockage des données, un lieu que le fournisseur de services choisit généralement sur la base de considérations légitimes telles que la sécurité des données, les économies d'échelle et la rapidité d'accès. Par conséquent, pour un nombre croissant d'affaires pénales portant sur toutes sortes d'actes criminels[1], les autorités des États membres doivent pouvoir accéder à des données susceptibles de servir de preuves et qui sont stockées à l'extérieur de leurs frontières et/ou par des fournisseurs de services établis dans d'autres États membres ou dans des pays tiers.

Pour ces cas où les preuves ou les fournisseurs de services se trouvent à l'étranger, des mécanismes de coopération ont été mis en place entre pays depuis plusieurs dizaines d'années[2]. Malgré de fréquentes réformes, ces mécanismes de coopération sont de plus en plus mis à rude épreuve face à la nécessité grandissante d'accéder rapidement aux preuves électroniques à l'étranger. Plusieurs États membres et pays tiers ont réagi en développant leurs outils nationaux. La fragmentation qui en découle engendre une insécurité juridique et des obligations contradictoires, et soulève des questions relatives à la protection des droits fondamentaux et des garanties procédurales pour les personnes concernées par ce type de demandes.

En 2016, le Conseil a réclamé des mesures concrètes fondées sur une approche européenne commune visant à rendre l'entraide judiciaire plus efficace; à améliorer la coopération entre les autorités des États membres et les fournisseurs de services établis dans des pays tiers; et à proposer des solutions au problème que pose la détermination de la compétence d'exécution[3] dans le cyberespace[4]. Le Parlement européen a également souligné les défis que le cadre

---

1 Voir les sections 2.1.1 et 2.3 de l'analyse d'impact.

2 Au sein de l'Union, des mécanismes de reconnaissance mutuelle, désormais fondés sur la directive concernant la décision d'enquête européenne. Avec les pays tiers, des mécanismes d'entraide judiciaire.

3 Dans le présent document, la notion de «compétence d'exécution» fait référence à la compétence des autorités concernées pour diligenter des mesures d'enquête.

4 Conclusions du Conseil de l'Union européenne sur l'amélioration de la justice pénale dans le cyberespace, ST9579/16.

juridique actuellement fragmenté pose aux fournisseurs de services qui cherchent à se conformer aux demandes des services répressifs, et a préconisé un cadre juridique européen garantissant les droits et les libertés de toutes les parties concernées[5].

La présente proposition cible le problème spécifique que posent la nature volatile des preuves électroniques et leur dimension internationale. Elle vise à adapter les mécanismes de coopération à l'ère numérique en fournissant les outils judiciaires et répressifs nécessaires pour tenir compte des modes de communication actuels des criminels et pour lutter contre les formes modernes de criminalité. De tels outils sont subordonnés à l'existence de solides mécanismes de protection des droits fondamentaux. La présente proposition vise à renforcer la sécurité juridique pour les autorités, les fournisseurs de services et les personnes concernées et à maintenir un niveau de qualité élevé pour les demandes des services répressifs, en garantissant la protection des droits fondamentaux, la transparence et l'obligation de rendre des comptes. Elle accélère également le processus pour recueillir et obtenir des preuves électroniques qui sont stockées et/ou détenues par des fournisseurs de services établis dans une autre juridiction. Cet instrument coexistera avec les instruments actuels de coopération judiciaire qui sont toujours pertinents et pourra le cas échéant être utilisé par les autorités compétentes. Parallèlement, la Commission s'efforce de renforcer les mécanismes de coopération judiciaire existants à l'aide de mesures telles que la création d'une plateforme sûre pour échanger rapidement les demandes entre les autorités judiciaires au sein de l'UE, et un investissement d'un million d'euros pour former des praticiens de tous les États membres de l'UE à l'entraide et à la coopération judiciaires, qui mettent l'accent sur les États-Unis (le troisième pays recevant le plus grand nombre de demandes émises par l'UE)[6].

Les autorités doivent pouvoir s'appuyer sur le représentant légal désigné par les fournisseurs de services pour la signification et l'exécution des décisions au titre du présent instrument. La Commission présente ce jour une proposition pour s'assurer que ces représentants légaux soient effectivement désignés. Elle prévoit une solution commune à l'échelle de l'Union pour remettre les décisions de justice aux fournisseurs de services par l'intermédiaire d'un représentant légal.

- **Cohérence par rapport au cadre juridique de l'UE dans le domaine d'action et par rapport à la convention de Budapest du Conseil de l'Europe**

Le cadre juridique actuel de l'UE se compose des instruments de coopération de l'Union en matière pénale, tels que la directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale[7], la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[8], la décision 2002/187/JAI du Conseil instituant Eurojust[9], le règlement (UE) 2016/794 relatif à Europol[10], la décision-cadre 2002/465/JAI du

5 P8_TA(2017)0366.

6 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

7 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.

8 Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.

9 Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité. En 2013, la Commission a adopté une proposition de règlement pour réformer Eurojust [Proposition de règlement du Parlement européen et du Conseil relatif à

Conseil relative aux équipes communes d'enquête[11], ainsi que les accords bilatéraux entre l'Union et les pays tiers, tels que l'accord sur l'entraide judiciaire entre l'Union européenne et les États-Unis[12] et celui entre l'Union et le Japon[13].

Par l'introduction d'injonctions européennes de production et de conservation, la proposition contribue à simplifier l'obtention et la collecte, dans le cadre de procédures pénales, des preuves électroniques qui sont stockées ou détenues par des fournisseurs de services relevant d'une autre juridiction. La directive concernant la décision d'enquête européenne en matière pénale, qui remplace dans une large mesure la convention relative à l'entraide judiciaire en matière pénale, couvre toutes les mesures d'enquête[14], y compris l'accès aux preuves électroniques, mais ne contient aucune disposition spécifique à ce type de preuves[15]. Le nouvel instrument ne remplacera pas la directive concernant la décision d'enquête européenne en ce qui concerne l'obtention de preuves électroniques, mais fournit un outil supplémentaire aux autorités. Par exemple, dans certaines situations qui requièrent la mise en œuvre de plusieurs mesures d'enquête dans l'État membre chargé de la mise en œuvre, les autorités pourraient choisir prioritairement de recourir à la décision d'enquête européenne. Il est préférable de créer un nouvel instrument pour les preuves électroniques plutôt que de modifier la directive concernant la décision d'enquête européenne en raison des difficultés spécifiques inhérentes à l'obtention des preuves électroniques qui n'ont pas d'incidence sur les autres mesures d'enquête prévues par la directive.

Le nouvel instrument s'appuiera sur les principes de reconnaissance mutuelle afin de faciliter la collecte transfrontière des preuves électroniques. Aucune autorité dans le pays de résidence du destinataire de l'injonction ne devra procéder directement à sa signification ni à son exécution, excepté en cas de non-conformité, auquel cas des mesures de mise en œuvre devront être prises et l'intervention de l'autorité compétente dans le pays où est établi le représentant sera nécessaire. L'instrument requiert par conséquent un ensemble de garanties et de dispositions solides, telles que la validation par une autorité judiciaire dans chaque cas. Par exemple, les injonctions européennes de production de données relatives aux transactions ou au contenu (contrairement aux données relatives aux abonnés et aux données relatives à l'accès) ne peuvent être émises que pour les infractions pénales passibles dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans, ou pour les infractions purement informatiques, relevant de la cybercriminalité ou liées au terrorisme telles que visées dans la proposition.

---

l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust), COM/2013/0535 final].

10 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI.

11 Décision-cadre 2002/465/JAI du Conseil du 13 juin 2002 relative aux équipes communes d'enquête.

12 Décision 2009/820/PESC du Conseil du 23 octobre 2009 concernant la conclusion, au nom de l'Union européenne, de l'accord d'extradition entre l'Union européenne et les États-Unis d'Amérique et de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique.

13 Décision du Conseil 2010/616/UE du 7 octobre 2010 relative à la conclusion de l'accord sur l'entraide judiciaire en matière pénale entre l'Union européenne et le Japon.

14 Excepté pour les équipes communes d'enquête (voir l'article 3 de la directive concernant la décision d'enquête européenne); tous les États membres ne participent pas à cette directive (Irlande et Danemark).

15 Excepté pour faire référence à l'identification d'une personne détentrice d'une adresse IP au titre de l'article 10, paragraphe 2, point e, auquel cas la double incrimination ne peut être invoquée comme motif de refus de reconnaître et exécuter la demande.

Les données personnelles couvertes par cette proposition sont protégées et ne peuvent être traitées qu'en accord avec le règlement général sur la protection des données (RGPD)[16] et la directive sur la protection des données destinées aux autorités policières et judiciaires pénales (directive relative à la protection des données dans un contexte répressif)[17]. Le RGPD entrera en application le 25 mai 2018, tandis que la directive relative à la protection des données dans un contexte répressif devra être transposée par les États membres pour le 6 mai 2018.

La convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest, CETS n° 185), ratifiée par la plupart des États membres de l'UE, établit des mécanismes internationaux de coopération dans la lutte contre la cybercriminalité[18]. Cette convention traite des crimes commis au moyen de l'internet et d'autres réseaux informatiques. Elle impose aussi aux parties d'établir les compétences et les procédures pour l'obtention des preuves électroniques et de s'assurer une entraide judiciaire non limitée à la cybercriminalité. La convention requiert notamment des parties d'établir des injonctions de production pour l'obtention de données informatiques auprès des fournisseurs de services établis sur leur territoire, et pour l'obtention des données relatives aux abonnés auprès de fournisseurs de services actifs sur leur territoire. En outre, la convention prévoit des injonctions de conservation lorsqu'il y a lieu de penser que les données informatiques sont particulièrement vulnérables à la perte ou aux modifications. La signification et l'application des injonctions nationales de production émises contre des fournisseurs établis en dehors du territoire d'une partie à la convention soulèvent d'autres questions. À cet égard, des mesures supplémentaires visant à améliorer l'accès transfrontière aux preuves électroniques sont actuellement à l'examen[19].

- **Résumé de la proposition de règlement**

La proposition de règlement introduit des injonctions européennes de production et de conservation contraignantes. Les deux injonctions doivent être émises ou validées par une autorité judiciaire d'un État membre. Une injonction peut être émise pour conserver ou produire des données stockées par un fournisseur de services situé dans une autre juridiction, et qui doivent servir de preuves dans le cadre d'enquêtes judiciaires ou de procédures pénales. Ces injonctions ne peuvent être émises que s'il existe une mesure similaire pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission. Les deux injonctions peuvent être signifiées aux fournisseurs de services de communications

---

16 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.

17 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.

18 Dans le cadre de la stratégie 2013 de l'Union européenne en matière de cybersécurité, la convention de Budapest a été reconnue comme le principal cadre multilatéral pour la lutte contre la cybercriminalité - Communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant une stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, JOIN(2013) 1 final.

19 Lors de sa 17e séance plénière (juin 2017), le comité de la convention sur la cybercriminalité (T-CY) a adopté le cahier des charges pour la préparation d'un deuxième protocole additionnel à la convention (le «deuxième protocole additionnel»), dont la version finale préparée par le T-CY est prévue pour décembre 2019. L'objectif consiste à réduire l'importance du facteur que constitue le lieu de stockage des données.

électroniques, réseaux sociaux, marchés en ligne, autres fournisseurs de services d'hébergement et fournisseurs d'infrastructures internet comme les registres d'adresses IP et de noms de domaine, ou à leurs représentants légaux le cas échéant. L'injonction européenne de conservation, à l'instar de l'injonction de production, est adressée au représentant légal hors de la juridiction de l'État membre d'émission afin de conserver les données en vue d'une demande ultérieure de production desdites données, par exemple au moyen des canaux d'entraide judiciaire dans le cas de pays tiers ou d'une décision d'enquête européenne entre des États membres participants. Contrairement aux mesures de surveillance ou aux obligations de conservation des données établies par la loi, lesquelles ne sont pas couvertes par le présent règlement, l'injonction européenne de conservation est une injonction émise ou validée par une autorité judiciaire dans le cadre d'une procédure pénale concrète, après évaluation de la proportionnalité et de la nécessité dans chaque cas particulier. À l'instar de l'injonction européenne de production, elle vise les auteurs connus ou inconnus d'une infraction pénale déjà commise. L'injonction européenne de conservation permet uniquement de conserver des données déjà stockées au moment de la réception de l'injonction, et non d'accéder aux données à une date postérieure à la réception.

Les deux injonctions ne peuvent servir que dans le cadre de procédures pénales, depuis la phase d'instruction préalable au procès jusqu'à la clôture de la procédure par voie de jugement ou d'une autre décision. Les injonctions de production de données relatives aux abonnés et de données relatives à l'accès peuvent être émises pour toutes les infractions pénales, tandis que les injonctions de production de données relatives aux transactions ou au contenu ne peuvent être émises que pour les infractions pénales passibles dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans ou pour les infractions spécifiques visées par la proposition, et lorsqu'il existe un lien particulier avec les outils et infractions électroniques visés par la directive 2017/541/UE relative à la lutte contre le terrorisme.

Compte tenu du caractère intrusif, à des degrés divers, des mesures imposées concernant les données requises, la proposition établit plusieurs conditions et garanties. Celles-ci comportent notamment l'obligation d'obtenir la validation préalable des injonctions par une autorité judiciaire. La proposition ne concerne que les données stockées. Elle ne couvre pas l'interception des télécommunications en temps réel. La mesure se limite aux données nécessaires et proportionnées aux fins des procédures pénales concernées. Elle permet également aux fournisseurs de services d'obtenir des éclaircissements auprès des autorités d'émission, le cas échéant. S'il est impossible de résoudre les problèmes et si l'autorité d'émission décide de prendre des mesures répressives, les fournisseurs de services peuvent avancer les mêmes motifs pour s'opposer à la mise en œuvre de ces mesures par leurs propres autorités. De plus, une procédure spécifique est prévue dans les cas où l'obligation de fournir des données est contraire à une obligation découlant de la législation d'un pays tiers.

La législation européenne protège les droits des suspects et des personnes poursuivies dans le cadre d'une procédure pénale, et des règles existent déjà pour assurer la protection des données à caractère personnel. Cependant, pour les personnes dont les données sont requises, les garanties supplémentaires contenues dans la proposition prévoient des droits procéduraux en leur faveur dans le cadre ou non de la procédure pénale. Ces droits comprennent la possibilité de contester la légalité, la nécessité ou la proportionnalité de l'injonction sans restriction des motifs de récusation conformément à la législation nationale. Le plein respect des droits au titre de la législation de l'État chargé de la mise en œuvre est assuré par la prise en considération, par l'État d'émission, des immunités et privilèges protégeant les données requises dans l'État membre du fournisseur de services. Cela vaut tout particulièrement dans

le cas où ces immunités et privilèges assurent une meilleure protection que la législation de l'État d'émission.

Les injonctions au titre du règlement proposé sont applicables aux mêmes conditions que les injonctions nationales comparables dans la juridiction où le fournisseur de services reçoit l'injonction. Le règlement prévoit que les États membres mettent en place des sanctions efficaces et proportionnées.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de l'action menée dans ce domaine est constituée par l'article 82, paragraphe 1, du traité sur le fonctionnement de l'Union européenne (traité FUE). L'article 82, paragraphe 1, prévoit que des mesures peuvent être adoptées conformément à la procédure législative ordinaire afin d'établir des règles et procédures pour assurer la reconnaissance de toutes les formes de jugements et de décisions judiciaires dans l'ensemble de l'Union. Des mesures peuvent également être adoptées afin de faciliter la coopération entre les autorités judiciaires ou équivalentes des États membres dans le cadre des poursuites pénales et de l'exécution des décisions.

Cette base juridique s'applique aux mécanismes couverts par le présent règlement. L'article 82, paragraphe 1, assure la reconnaissance mutuelle des décisions adoptées par une autorité judiciaire dans l'État d'émission à l'égard d'une personne morale dans un autre État membre, voire même lui imposant des obligations, sans l'intervention préalable d'une autorité judiciaire dans cet autre État membre. L'injonction européenne de production ou de conservation peut conduire si nécessaire à l'intervention d'une autorité judiciaire de l'État chargé de la mise en œuvre pour faire appliquer la décision.

• Choix de l'instrument

L'article 82, paragraphe 1, du traité FUE offre la possibilité au législateur de l'Union d'adopter des règlements et des directives.

Étant donné que que la proposition concerne des procédures transfrontières exigeant des règles uniformes, il est inutile de laisser une marge aux États membres pour transposer ces règles. Un règlement est directement applicable, est gage de clarté et de sécurité juridique renforcée, et évite les interprétations divergentes par les États membres et d'autres problèmes de transposition rencontrés avec les décisions-cadres relatives à la reconnaissance mutuelle des jugements et décisions judiciaires. En outre, un règlement permet d'imposer une même obligation uniformément au sein de l'Union. Par conséquent, la forme jugée la plus appropriée pour cet instrument de reconnaissance mutuelle est celle du règlement.

• Subsidiarité

Compte tenu de la dimension transfrontière des problèmes abordés, les mesures prévues dans la proposition doivent être adoptées au niveau de l'Union afin d'atteindre les objectifs visés. Les infractions pour lesquelles il existe des preuves électroniques sont souvent commises lorsque l'infrastructure de stockage des preuves électroniques et le fournisseur de services exploitant ladite infrastructure relèvent d'un cadre juridique national différent, au sein ou en dehors de l'Union, de celui de la victime ou de l'auteur de l'infraction. Par conséquent, accéder effectivement à des preuves électroniques hors de ses frontières peut s'avérer long et complexe pour le pays compétent en l'absence de règles communes minimales. Les États

membres agissant isolément rencontreraient des difficultés pour relever notamment les défis suivants:

- la fragmentation des cadres juridiques au sein des États membres, reconnue comme un problème majeur par les fournisseurs de services cherchant à se conformer aux demandes basées sur différentes lois nationales;
- une coopération judiciaire plus rapide sur la base de la législation européenne existante, notamment au moyen de la décision d'enquête européenne.

En raison de la diversité des approches juridiques, du nombre de domaines concernés (sécurité, droits fondamentaux y compris droits procéduraux et protection des données à caractère personnel, questions économiques), et du large éventail d'intervenants, une législation à l'échelle de l'Union constitue le meilleur moyen de remédier aux problèmes constatés.

- **Proportionnalité**

La proposition énonce des règles permettant à une autorité compétente de l'Union d'imposer à un fournisseur de services exerçant ses activités dans l'Union mais établi dans un autre État membre de produire ou de conserver des preuves électroniques. Les caractéristiques clés de la proposition — à savoir le champ d'application matériel de l'injonction européenne de production, les conditions pour garantir la courtoisie, le mécanisme de sanction et le système de garanties et de recours légaux — limitent celle-ci au strict nécessaire pour atteindre ses principaux objectifs. La proposition se limite notamment aux demandes de données stockées (les données issues de l'interception en temps réel des télécommunications ne sont pas couvertes) et aux injonctions émises dans le cadre de procédures pénales pour une infraction pénale spécifique faisant l'objet d'une enquête en cours. Elle ne couvre donc pas la prévention de la criminalité ni d'autres types de procédures ou d'infractions (telles que des procédures administratives pour infractions aux règles de droit) et n'impose pas aux fournisseurs de recueillir et de conserver systématiquement plus de données que celles nécessaires pour des motifs commerciaux ou de conformité avec d'autres exigences légales. En outre, alors que les injonctions de production de données relatives aux abonnés et de données relatives à l'accès peuvent être émises pour toutes les infractions pénales, les injonctions de production de données relatives aux transactions ou au contenu ne peuvent être émises que pour les infractions pénales passibles dans l'État d'émission d'une peine privative de liberté d'une durée maximale d'au moins trois ans, ou pour les infractions purement informatiques, relevant de la cybercriminalité ou liées au terrorisme définies dans la proposition. Enfin, la proposition clarifie les règles et garanties de procédure applicables en matière d'accès transfrontière aux preuves électroniques, sans aller jusqu'à exiger une harmonisation des mesures nationales. Elle se limite à ce qui est nécessaire et proportionné pour satisfaire aux besoins des services répressifs et des autorités judiciaires à l'ère numérique.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Consultation des parties intéressées**

Pendant un an et demi, la Commission a consulté tous les intervenants concernés afin de déceler les problèmes et aller de l'avant. Elle a procédé à l'aide d'enquêtes, allant des consultations publiques ouvertes aux enquêtes ciblées auprès des autorités publiques concernées. Des réunions de groupes d'experts et des réunions bilatérales ont également été organisées pour examiner les effets potentiels de la législation de l'Union. Des conférences

consacrées à l'accès transfrontière aux preuves électroniques ont quant à elles permis de recueillir des avis sur cette initiative.

Dans l'ensemble, les personnes interrogées ont jugé l'utilisation croissante des services d'information problématique en matière d'application de la loi, étant donné le manque général de moyens des autorités compétentes pour traiter les preuves en ligne. Le processus fastidieux d'obtention des preuves est également considéré comme l'un des principaux obstacles. Les autres problèmes majeurs mis en avant par les autorités publiques comprennent notamment le manque de coopération fiable avec les fournisseurs de services, le manque de transparence et l'insécurité juridique liée aux compétences relatives aux moyens d'investigation. Une coopération transfrontière directe entre les services répressifs et les fournisseurs de services numériques devrait contribuer à faciliter les enquêtes judiciaires. Les fournisseurs de services et certaines organisations de la société civile ont témoigné de la nécessité d'assurer la sécurité juridique en cas de coopération avec les autorités publiques et d'éviter les conflits de lois. Pour ce qui est des inquiétudes relatives aux conséquences que la nouvelle législation de l'UE pourrait avoir sur les droits, les parties intéressées ont estimé nécessaire l'application de garanties spécifiques pour tout instrument transfrontière.

Les avis recueillis lors de l'analyse d'impact initiale indiquaient que selon les parties intéressées, combler les lacunes du système actuel d'entraide judiciaire améliorerait son efficacité et la sécurité juridique. Certaines organisations de la société civile se sont opposées à la coopération directe prévue par la législation de l'Union. Elles préféraient limiter l'action de l'Union à l'amélioration des procédures d'entraide juridique. Cette idée sera développée dans le cadre des mesures pratiques approuvées par le Conseil en juin 2016.

Une enquête ciblant les autorités publiques dans les États membres a révélé l'absence d'approche commune pour l'obtention d'un accès transfrontière aux preuves électroniques, étant donné que chaque État membre suit ses propres pratiques internes. De même, les fournisseurs de services réagissent différemment aux demandes émises par les services répressifs étrangers, et les temps de réponse varient selon l'État membre à l'origine de la demande. Cette situation est source d'insécurité juridique pour toutes les parties intéressées impliquées.

La consultation des parties intéressées a, de manière générale, révélé que le cadre juridique actuel est fragmenté et complexe. Cela peut entraîner des retards lors de la phase d'exécution, et compromettre l'efficacité des enquêtes et poursuites judiciaires nécessitant l'accès transfrontière à des preuves électroniques.

- **Analyse d'impact**

Le comité d'examen de la réglementation a émis un avis favorable sur l'analyse d'impact appuyant la présente proposition[20] ainsi que diverses suggestions pour l'améliorer[21]. À la

[20] Document de travail des services de la Commission – Analyse d'impact joint à la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et à la proposition de directive définissant des règles harmonisées pour la désignation de représentants légaux en vue de collecter des preuves dans le cadre de procédures pénales, SWD(2018) 118.

[21] Comité d'examen de la réglementation de la Commission européenne – Avis sur l'analyse d'impact – Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et à la proposition de directive définissant des règles

suite de cet avis, l'analyse d'impact a été modifiée pour traiter davantage les questions de droits fondamentaux liées au partage transfrontière de données, notamment les liens entre les diverses mesures constituant l'option retenue. Des modifications ont également été apportées afin que l'analyse reflète mieux les opinions des parties intéressées et des États membres ainsi que la façon dont elles ont été prises en considération. De plus, le contexte stratégique a été revu pour inclure des références supplémentaires aux divers aspects tels que des discussions de groupes d'experts qui ont contribué à donner forme à l'initiative. La complémentarité des différentes mesures (notamment la directive relative à la décision d'enquête européenne, les négociations concernant un protocole additionnel à la convention de Budapest et l'examen conjoint de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis) a été mieux définie en termes de champ d'application, de calendrier et de portée, et le scénario de base a été corrigé pour mieux refléter les développements susceptibles de se produire indépendamment de l'adoption des mesures proposées. Pour conclure, des ordinogrammes ont été ajoutés afin de mieux décrire les processus de partage de données.

Quatre options principales ont été envisagées en plus du scénario de base (option O): plusieurs mesures pratiques visant à améliorer à la fois les procédures de coopération judiciaire et la coopération directe entre les autorités publiques et les fournisseurs de services (option A: non législative); une option combinant les mesures pratiques de l'option A avec des solutions internationales à un niveau bilatéral ou multilatéral (option B: législative); une option combinant les mesures prévues par l'option B avec une injonction européenne de production et une mesure visant à améliorer l'accès aux bases de données pour répondre aux demandes d'informations relatives aux abonnés, par exemple la base WHOIS de noms de domaine (option C: législative); et une option combinant toutes les mesures précédentes prévues par l'option C avec une législation encadrant l'accès direct aux données conservées à distance (option D: législative)[22].

Si aucune mesure n'est prise (option O), le nombre croissant de demandes rendra la situation encore pire. Toutes les autres options contribuent à atteindre les objectifs visés par l'initiative, mais à des degrés divers. L'option A permettrait d'améliorer l'efficacité des processus actuels, par exemple en améliorant la qualité des demandes, mais selon une marge qui serait limitée par les lacunes structurelles du système actuel.

L'option B garantirait davantage d'améliorations grâce à des solutions acceptées à l'échelle internationale, mais dont les résultats dépendraient largement des pays tiers. Il est donc peu probable que ces solutions incertaines soient efficaces et offrent autant de garanties qu'une solution à l'échelle de l'Union.

L'option C apporte une valeur ajoutée évidente par rapport aux options précédentes en prévoyant également à l'intérieur de l'Union un instrument de coopération directe avec les fournisseurs de services comme solution à la plupart des problèmes rencontrés lorsqu'un fournisseur de services détient les données concernées.

---

harmonisées pour la désignation de représentants légaux en vue de collecter des preuves dans le cadre de procédures pénales, SEC(2018) 199.

22 Pour de plus amples informations, voir le document de travail des services de la Commission – Analyse d'impact joint à la proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et à la proposition de directive définissant des règles harmonisées pour la désignation de représentants légaux en vue de collecter des preuves dans le cadre de procédures pénales, SWD(2018) 118.

L'option D constitue la solution la plus complète. Outre les mesures précédentes, elle prévoit une mesure législative d'accès direct lorsque la contribution d'un fournisseur de services n'est pas nécessaire.

La présente initiative législative que propose la Commission est fondée sur les conclusions de l'analyse d'impact. Cet acte législatif sera complété par des mesures pratiques décrites dans l'analyse d'impact et par des travaux constants visant à créer un protocole additionnel à la convention de Budapest. Sur la base de sa proposition législative, la Commission examinera également avec les États-Unis et d'autres pays tiers la possibilité de conclure ultérieurement des accords bilatéraux ou multilatéraux concernant l'accès transfrontière à des preuves électroniques intégrant les garanties nécessaires. Pour les mesures d'accès direct et d'accès à des bases de données dont il est question dans l'option D, la Commission n'a proposé aucun acte législatif pour le moment, mais se penchera plus tard sur le meilleur moyen de régler ces deux questions.

L'initiative devrait donner lieu à des enquêtes et poursuites plus efficaces tout en améliorant la transparence et l'obligation de rendre compte, ainsi que le respect des droits fondamentaux. Elle devrait également renforcer la confiance dans le marché numérique unique en renforçant la sécurité et en réduisant le sentiment d'impunité des crimes commis sur ou au moyen de dispositifs en réseau.

Il est prévu que cette initiative génère des coûts initiaux de mise en œuvre pour les autorités publiques, lesquels seront compensés à long terme par les économies au niveau des coûts récurrents. Les autorités nationales devront s'adapter aux nouvelles procédures et suivre des formations. Cependant, elles pourront ensuite bénéficier de l'harmonisation et de la centralisation d'un cadre juridique plus clair régissant les demandes d'accès aux données, qui permettront de gagner en efficacité. De même, puisque l'option retenue soulagerait la pression subie par les canaux de coopération judiciaire, les pays destinataires des demandes devraient constater une diminution du nombre de demandes à traiter.

Les fournisseurs de services devront s'adapter à un nouveau cadre législatif par la mise en place de (nouvelles) procédures et la formation de leur personnel. En revanche, un cadre harmonisé pourrait réduire la charge de ces fournisseurs qui répondent actuellement aux demandes de données hors contenu et doivent les analyser en tenant compte des différentes législations de tous les États membres. La sécurité juridique et la normalisation des procédures devraient aussi avoir une incidence positive sur les petites et moyennes entreprises en allégeant la charge administrative et en favorisant la concurrence. De manière générale, cette initiative devrait également leur permettre de faire des économies.

- **Droits fondamentaux**

La proposition risquerait éventuellement de compromettre plusieurs droits fondamentaux:

- les droits des personnes dont les données sont consultées: le droit à la protection des données à caractère personnel; le droit au respect de la vie privée et familiale; le droit à la liberté d'expression; les droits de la défense; le droit à un recours effectif et à accéder à un tribunal impartial;
- les droits du fournisseur de services: le droit à la liberté d'entreprise; le droit à un recours effectif;
- les droits de tous les citoyens: le droit à la liberté et à la sûreté.

Compte tenu de l'acquis en matière de protection des données, des garanties suffisantes et considérables ont été ajoutées à la proposition de règlement afin d'assurer la protection des droits de ces personnes.

Vu que les injonctions ne peuvent être émises que dans le cadre de procédures pénales et à condition que des situations comparables existent au niveau national, tant lors de la phase préalable au procès que durant le procès, toutes les garanties procédurales en matière de droit pénal sont applicables. Ces garanties comprennent notamment le droit à accéder à un tribunal impartial consacré à l'article 6 de la CEDH et aux articles 47 et 48 de la Charte des droits fondamentaux. Elles comprennent aussi la législation correspondante à l'échelle de l'Union sur les droits procéduraux en matière de procédures pénales: la directive 2010/64/UE relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales, la directive 2012/13/UE relative au droit aux informations relatives aux droits et à l'accusation et à l'accès au dossier de l'affaire, la directive 2013/48/UE relative au droit d'accès à un avocat dans le cadre des procédures pénales et au droit à la communication avec les proches lors de l'arrestation et de la détention, la directive 2016/343 portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès, la directive 2016/800 relative à la mise en place de garanties procédurales en faveur des enfants et la directive 2016/1919 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.

Plus particulièrement, l'intervention préalable d'une autorité judiciaire lors de l'émission d'une injonction garantit que la légalité de la mesure, ainsi que sa nécessité et sa proportionnalité par rapport à l'affaire en cause ont été vérifiées. Elle permet également d'éviter que l'injonction n'empiète indûment sur les droits fondamentaux, y compris les effets de principes de droit tels que le privilège des confidences à l'avocat. L'autorité d'émission doit s'assurer dans chaque cas que la mesure est nécessaire et proportionnée, notamment au vu de la gravité de l'infraction faisant l'objet de l'enquête. La proposition prévoit également des seuils pour les données relatives aux transactions et au contenu afin que l'injonction européenne de production ne soit utilisée que pour les formes d'infractions les plus graves par rapport auxdites données.

De plus, la proposition aborde explicitement le droit à un recours effectif pour les personnes dont les données sont requises. Les immunités et les privilèges liés à certaines professions, par exemple celle d'avocat, ainsi que les intérêts fondamentaux de sécurité ou de défense nationales dans l'État du destinataire doivent aussi être pris en considération lors du procès dans l'État d'émission. L'examen par une autorité judiciaire constitue ici une garantie supplémentaire.

L'injonction représentant une mesure contraignante, elle influence également les droits des fournisseurs de services, notamment leur liberté d'entreprise. La proposition reconnaît au fournisseur de services le droit de soulever certaines revendications dans l'État membre d'émission, par exemple dans le cas où l'injonction n'a pas été émise ou validée par une autorité judiciaire. Si l'injonction est renvoyée pour application à l'État chargé de la mise en œuvre, l'autorité chargée de la mise en œuvre peut décider de ne pas reconnaître ou de ne pas mettre en œuvre l'injonction si des motifs limités de refus apparaissent au moment de sa réception, et après consultation de l'autorité d'émission. En outre, si la procédure de mise en œuvre est tout de même lancée, le destinataire peut lui-même s'opposer à l'injonction devant l'autorité chargée de la mise en œuvre sur la base de ces motifs limités. Sont notamment concernés les cas où il apparaît que l'injonction n'est pas émise ou validée par une autorité

compétente, ou si son application constitue une violation manifeste de la Charte ou est clairement abusive. Cela n'exclut pas le droit du destinataire à un recours judiciaire effectif contre une décision imposant une sanction.

Le problème que les mesures de l'UE pourraient poser dans ce domaine est la possibilité que des pays tiers introduisent des obligations réciproques pour les fournisseurs de services qui manqueraient de cohérence avec les conditions de l'Union relatives aux droits fondamentaux, notamment le niveau élevé de protection des données garanti par l'acquis de l'Union. La proposition résout ce problème de deux façons: premièrement, en définissant une mesure qui prévoit de solides garanties et des références explicites aux conditions et garanties déjà inhérentes à l'acquis de l'UE, et qui pourra servir de modèle pour les législations étrangères; et deuxièmement, en ajoutant une clause spécifique pour les «obligations contradictoires» qui permettrait aux fournisseurs de services de repérer et signaler les obligations contradictoires auxquelles ils font face, et de solliciter un contrôle juridictionnel. Cette clause vise à garantir le respect des lois générales de blocage, par exemple l'Electronic Communications Privacy Act américain (loi sur la confidentialité des communications électroniques, ECPA) qui interdit la divulgation de données relatives au contenu dans sa zone géographique excepté dans des circonstances limitées, ainsi que des lois qui n'interdisent pas la divulgation de manière générale mais peuvent le faire dans certains cas particuliers. Pour les affaires relevant de l'ECPA, l'accès aux données relatives au contenu peut actuellement être interdit dans certaines situations, et l'entraide judiciaire constituera donc l'outil principal pour accéder à ces données. Cependant, en raison des modifications découlant de l'adoption du CLOUD Act américain[23] — la loi visant à clarifier l'utilisation légale des données à l'étranger — un accord entre l'UE et les États-Unis permettrait de suspendre la loi de blocage. Des accords internationaux supplémentaires avec d'autres partenaires clés permettraient de réduire davantage les situations de conflit de lois.

Compte tenu de ce qui précède, les mesures avancées dans cette proposition sont compatibles avec les droits fondamentaux.

4. INCIDENCE BUDGÉTAIRE

La proposition législative de règlement n'a aucune influence sur le budget de l'Union.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Le règlement est directement applicable au sein de l'Union. Il sera appliqué directement par les praticiens sans aucune modification des systèmes juridiques internes.

Le règlement sera soumis à évaluation et la Commission soumettra un rapport au Parlement européen et au Conseil au plus tard cinq ans après son entrée en vigueur. Sur la base des conclusions du rapport, notamment sur les vides éventuellement laissés par le règlement dans la pratique, et eu égard aux progrès technologiques, la Commission évaluera la nécessité d'élargir son champ d'application. S'il y a lieu, la Commission présentera des propositions visant à adapter le présent règlement. Les États membres fourniront à la Commission les

[23] La loi visant à clarifier l'utilisation légale des données à l'étranger (CLOUD Act) a été adoptée le 23 mars 2018 aux États-Unis. Le CLOUD Act est disponible ici.

informations nécessaires à l'établissement du rapport. Les États membres compileront les données nécessaires au contrôle annuel de l'application du règlement.

Le cas échéant, la Commission fournira des recommandations aux fournisseurs de services qui cherchent à se conformer à leurs obligations au titre du règlement.

- **Explication détaillée des différentes dispositions de la proposition**

	RÈGLEMENT	
	Article	**Considérant**
I. Objet, définitions et champ d'application	1. Objet	1-15
	2. Définitions	16-23
	3. Champ d'application	24-27
II. Injonction européenne de production, injonction européenne de conservation et certificats, représentant légal	4. Autorité d'émission	30
	5. Conditions d'émission d'une injonction européenne de production	28-29, 31-35
	6. Conditions d'émission d'une injonction européenne de conservation	36
	7. Destinataire d'une injonction européenne de production et d'une injonction européenne de conservation	37
	8. Certificat d'injonction européenne de production et certificat d'injonction européenne de conservation	38-39
	9. Exécution d'un EPOC	40-41
	10. Exécution d'un EPOC-PR	42
	11. Confidentialité et information de l'utilisateur	43
	12. Remboursement des frais	Néant
III. Sanctions et exécution	13. Sanctions	Néant
	14. Procédure de mise en œuvre	44-45, 55
IV. Voies de recours	15. et 16. Procédure de réexamen en cas d'obligations contradictoires découlant de la législation d'un pays tiers	47-53
	17. Recours effectifs	54

	18. Garantie des privilèges et des immunités en vertu du droit de l'État chargé de la mise en œuvre	35
V. Dispositions finales	19. Suivi et rapports	58
	20. Modifications des certificats et des formulaires	59-60
	21. Exercice de la délégation	60
	22. Notifications	Néant
	23. Rapport avec les décisions d'enquête européennes	61
	24. Évaluation	62
	25. Entrée en vigueur	Néant

Chapitre 1: Objet, définitions et champ d'application

Article premier: Objet

Le présent article établit le champ d'application général et le but de la proposition, à savoir fixer les règles en vertu desquelles une autorité judiciaire compétente au sein de l'Union européenne peut imposer à un fournisseur de services actif dans l'Union de produire ou de conserver des preuves électroniques au moyen d'une injonction européenne de production ou de conservation. Ces instruments ne peuvent être utilisés que dans des situations transfrontières, c'est-à-dire lorsque le fournisseur de services est établi ou représenté dans un autre État membre.

Le règlement fournit des outils supplémentaires aux autorités chargées des enquêtes pour obtenir des preuves électroniques sans limiter les pouvoirs déjà prévus par la législation nationale pour contraindre les fournisseurs de services établis ou représentés sur leur territoire. Si le fournisseur de services est établi ou représenté dans le même État membre, les autorités de cet État membre ont alors recours à des mesures nationales pour contraindre le fournisseur.

Les données requises au moyen d'une injonction européenne de production doivent être transmises directement aux autorités sans l'intervention des autorités de l'État membre où est établi ou représenté le fournisseur de services. Le règlement abandonne également la localisation des données comme facteur de connexion déterminant, étant donné que le stockage n'implique aucun contrôle de la part de l'État au sein duquel les données sont stockées. Les conditions de stockage des données sont généralement déterminées par le fournisseur sur la base de considérations commerciales[24].

[24] L'analyse d'impact fournit de plus amples explications.

De plus, le règlement s'applique également si les fournisseurs de services ne sont pas établis ou représentés au sein de l'Union mais y proposent pourtant leurs services. Cette disposition se retrouve à l'article 3, paragraphe 1.

Lorsque la proposition fait référence à un fournisseur de services établi ou représenté dans un État membre par un représentant légal désigné, le seul fait de désigner un représentant légal ne revient pas à créer un établissement du fournisseur de services aux fins du présent règlement.

L'article premier, paragraphe 2, n'a pas pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques consacrés par l'article 6 du traité sur l'Union européenne.

Article 2: Définitions

Cet article établit les définitions pour tout l'instrument.

Les types suivants de fournisseurs de services entrent dans le champ d'application du règlement: les fournisseurs de services de communications électroniques, les fournisseurs de services de sociétés d'informations pour qui le stockage de données est un composant déterminant du service fourni à l'utilisateur, y compris les réseaux sociaux dans la mesure où ils ne sont pas considérés comme des services de communications électroniques, les marchés en ligne permettant des transactions entre leurs utilisateurs (consommateurs ou entreprises) et les autres fournisseurs de services d'hébergement, ainsi que les fournisseurs de services de noms de domaine et de numérotation internet.

Le champ d'application du règlement couvre les fournisseurs de services de communications électroniques au sens de [la directive établissant le code des communications électroniques européen]. Concernant les services traditionnels de télécommunications, les particuliers et entreprises recourent de plus en plus, pour leurs communications interpersonnelles, à de nouveaux services sur l'internet, comme la voix sur IP, la messagerie instantanée et le courrier électronique web, en lieu et place des services de communication traditionnels. Ces services, ainsi que les réseaux sociaux tels Twitter et Facebook, sur lesquels les utilisateurs partagent du contenu, devraient donc aussi être couverts par cette proposition.

Dans de nombreux cas, les données ne sont plus stockées ou traitées sur le dispositif d'un utilisateur, mais rendues disponibles sur une infrastructure en nuage pour un accès à partir de n'importe quel endroit. Les fournisseurs de services n'ont pas besoin d'être établis ni de disposer de serveurs dans chaque juridiction, et se contentent d'une administration centralisée avec des systèmes décentralisés pour stocker les données et fournir leurs services. Ils procèdent de la sorte afin d'optimiser la répartition des charges et de réduire les délais de réponse aux demandes de données soumises par les utilisateurs. Les réseaux de diffusion de contenu (CDN) sont généralement déployés pour accélérer la diffusion de contenu en le copiant sur plusieurs serveurs répartis partout dans le monde. Les sociétés peuvent ainsi fournir du contenu à partir du serveur le plus proche de l'utilisateur ou capable d'acheminer la communication à travers le réseau le moins congestionné. Pour tenir compte de ce progrès, la définition couvre les services en nuage et autres services d'hébergement proposant une variété de ressources informatiques telles que des réseaux, serveurs ou autres infrastructures, services d'archivage, applications et services permettant d'archiver des données à diverses fins. L'instrument s'applique également aux marchés numériques qui permettent aux consommateurs et/ou aux entreprises de conclure des transactions par l'intermédiaire de

ventes ou contrats de services en ligne. Ces transactions sont effectuées soit sur le site web du marché en ligne, soit sur le site web d'un opérateur de marché qui utilise les services informatiques fournis par le marché en ligne. Par conséquent, ce marché en ligne est l'entité qui possède les preuves électroniques susceptibles d'être nécessaires dans le cadre de procédures pénales.

Les services qui n'incluent pas le stockage de données comme composant déterminant ne sont pas couverts par la proposition. Bien que la plupart des services fournis par les fournisseurs nécessitent de conserver certaines données, en particulier pour les services fournis à distance en ligne, ceux pour qui le stockage de données ne constitue pas une caractéristique principale et n'est donc que de nature accessoire, peuvent être traités à part, y compris les services juridiques, architecturaux, d'ingénierie et de comptabilité fournis à distance en ligne.

Les données que détiennent les fournisseurs de services d'infrastructures internet, tels que les registraires et registres de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire, ou les registres internet pour les adresses IP, peuvent être importantes dans le cadre de procédures pénales et fournir des indices conduisant à l'identification d'une personne ou d'une entité mêlée à des activités criminelles.

Les catégories de données que permet d'obtenir une injonction européenne de production émise par les autorités compétentes comprennent les informations relatives aux abonnés, les données relatives à l'accès, les données relatives aux transactions (les trois catégories étant généralement appelées collectivement les 'données hors contenu') et les données relatives au contenu stockées. Cette distinction, en dehors des données relatives à l'accès, existe dans les décisions juridiques de nombreux États membres, ainsi que dans des cadres juridiques de pays tiers.

Toutes les catégories contiennent des données à caractère personnel et sont par conséquent couvertes par les garanties au titre de l'acquis de l'UE relatif à la protecion des données. Les conséquences sur les droits fondamentaux ont une ampleur variable selon les catégories, en particulier entre les informations relatives aux abonnés d'une part, et les données relatives aux transactions et celles relatives au contenu d'autre part. Il est essentiel que l'instrument couvre ces trois catégories: les informations relatives aux abonnés et les données relatives à l'accès sont souvent source d'indices utiles pour une enquête visant à identifier un suspect. Tandis que les données relatives aux transactions et celles relatives au contenu peuvent fournir les preuves les plus probantes. En raison des différents niveaux d'interférence avec les droits fondamentaux, il convient d'assortir de différentes conditions les informations relatives aux abonnés d'une part, et les données relatives aux transactions et celles relatives au contenu d'autre part, comme prévu par plusieurs dispositions du règlement.

Il y a donc lieu de distinguer les données relatives à l'accès par une catégorie de données spécifique utilisée dans le présent règlement. Les données relatives à l'accès au sens de la présente sont recherchées dans le même but que les informations relatives aux abonnés, c'est-à-dire pour identifier l'utilisateur, et leur niveau d'interférence avec les droits fondamentaux est similaire. Elles doivent donc être soumises aux mêmes conditions que les informations relatives aux abonnés. C'est la raison pour laquelle cette proposition introduit une nouvelle catégorie de données qu'il faudra traiter comme des informations relatives aux abonnés si le même objectif est visé.

L'article 2 détermine les États membres et autorités susceptibles de participer à la procédure. L'article 4 fournit une définition de l'autorité d'émission.

Les cas d'urgence sont des situations exceptionnelles qui exigent souvent une réaction rapide des fournisseurs de services et sont soumises à des conditions spéciales. Ils sont donc définis séparément dans cet article.

Article 3: Champ d'application

Cet article définit le champ d'application de la proposition. Le règlement s'applique à tous les fournisseurs qui proposent leurs services au sein de l'Union européenne, notamment les fournisseurs établis en dehors de son territoire. L'offre active de services au sein de l'Union, avec tous les avantages qui en découlent, justifie l'application du règlement à ces fournisseurs de services et crée des conditions de concurrence équitables entre les participants d'un même marché. Par ailleurs, si ces fournisseurs n'étaient pas couverts, la faille qui en résulterait permettrait aux criminels de contourner facilement le champ d'application du règlement.

Pour déterminer si des services sont proposés, les autorités doivent vérifier si le fournisseur de services permet à des personnes morales ou physiques d'utiliser lesdits services dans un ou plusieurs États membres. Cependant, la simple possibilité d'accès à ces services (même via la possibilité d'accéder au site web du fournisseur de services ou d'un intermédiaire, ou par une adresse de courrier électronique ou d'autres coordonnées) ne constitue pas une condition suffisante à l'application de ce règlement. Un lien étroit avec ces États membres est donc nécessaire afin de garantir une connexion suffisante entre le fournisseur et le territoire sur lequel il propose ses services. Ce lien étroit existe lorsqu'un fournisseur de services possède un établissement dans un ou plusieurs États membres. En l'absence d'un établissement au sein de l'Union, le critère de lien étroit avec celle-ci est alors évalué sur la base du nombre d'utilisateurs dans un ou plusieurs États membres, ou du fait que les activités ciblent un ou plusieurs États membres. Le ciblage des activités vers un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, notamment des facteurs tels que le recours à une langue ou une monnaie généralement utilisées dans cet État membre ou la possibilité de commander des biens ou des services. Un État membre peut également être ciblé par des activités par le biais de la disponibilité d'une application dans la boutique d'applications nationale concernée, par la diffusion de publicités locales ou dans la langue officielle de l'État membre, par l'utilisation des informations issues de personnes dans des États membres dans le cadre de leurs activités, ou par le traitement des relations clientèle par exemple en proposant un service clientèle dans la langue généralement utilisée dans un État membre. Un lien substantiel doit également être établi lorsqu'un fournisseur de services oriente ses activités vers un ou plusieurs États membres tel qu'énoncé à l'article 17, paragraphe l, point c), du règlement 1215/2012 relatif à la compétence, à la reconnaissance et à l'exécution des décisions en matière civile et commerciale.

L'injonction européenne de production et l'injonction européenne de conservation sont des mesures d'enquête qui ne peuvent être émises que dans le cadre d'enquêtes judiciaires ou procédures pénales pour des infractions pénales réelles. Le lien avec une enquête réelle les distingue des mesures préventives ou obligations de conservation de données prévues par la loi et garantit l'application des droits procéduraux applicables aux procédures pénales. Par conséquent, la compétence d'ouverture d'enquêtes pour une infraction particulière est une condition préalable à l'utilisation du règlement.

À titre d'exigence supplémentaire, les données requises doivent être liées aux services proposés par le fournisseur au sein de l'Union.

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

Article 4: Autorité d'émission

Pour émettre une injonction européenne de production ou de conservation, l'autorité judiciaire doit être concernée soit en qualité d'autorité d'émission, soit de validation. Pour les injonctions de production portant sur des données relatives aux transactions ou sur celles relatives au contenu, l'intervention d'un juge ou d'une juridiction est requise. En ce qui concerne les informations relatives aux abonnés et les données relatives à l'accès, l'intervention d'un procureur convient également.

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

L'article 5 fixe les conditions d'émission d'une injonction européenne de production. L'autorité judiciaire d'émission est chargée de les vérifier.

L'injonction européenne de production ne peut être émise que si elle est nécessaire et proportionnée au cas particulier concerné. De plus, elle ne doit l'être que s'il existe une mesure similaire pour une situation nationale comparable dans l'État d'émission.

Les injonctions de production portant sur les informations relatives aux abonnés et les données relatives à l'accès peuvent être émises pour toutes les infractions pénales. Les données relatives aux transactions et celles relatives au contenu doivent faire l'objet d'exigences plus strictes pour refléter leur nature plus sensible et leur degré proportionnellement plus élevé d'intrusion par rapport aux deux catégories précédentes de données. Ces injonctions ne peuvent donc être émises que pour des infractions passibles d'une peine privative de liberté d'une durée maximale d'au moins trois ans ou plus. Une approche plus proportionnée est possible grâce au seuil constitué par la peine privative de liberté maximale, en complément de plusieurs conditions et garanties ex ante et ex post visant à garantir le respect du principe de proportionnalité et des droits des personnes concernées.

En revanche, un seuil ne doit pas compromettre l'efficacité de l'instrument ni son utilisation par les praticiens. Les États membres appliquent des seuils de peines différents en fonction de leur système national. Les codes pénaux nationaux diffèrent et ne sont pas harmonisés. Tel est le cas pour les infractions pénales et les sanctions qu'elles entraînent. Les codes procéduraux nationaux diffèrent également en ce qui concerne les seuils pour l'obtention de données relatives aux transactions ou de celles relatives au contenu: certains États membres ne fixent aucun seuil particulier; d'autres ont établi une liste d'infractions. Un seuil de trois ans limite le champ d'application de l'instrument aux infractions plus graves, sans restreindre de façon excessive ses possibilités d'utilisation à disposition des praticiens. Ce seuil exclut du champ d'application un large éventail d'infractions en fonction du code pénal de l'État membre (par exemple, dans certains États membres, la participation aux activités d'un groupe criminel organisé et l'enlèvement, mais également les infractions telles que le menu larcin, la fraude et les voies de fait pour lesquels une injonction de production transfrontière pour des données plus sensibles peut être jugée disproportionnée). Par ailleurs, un seuil de trois ans inclut les infractions requérant une approche plus efficace, telles que l'appartenance à une organisation criminelle, le financement de groupes terroristes, le soutien ou la promotion d'une organisation criminelle, la formation dans le but de commettre des infractions terroristes, certaines infractions perpétrées dans un but terroriste, et la préparation d'une infraction envisagée dans un but terroriste, ou la préparation d'une prise d'otages, qui serait autrement

exclue dans le cas d'un seuil plus élevé dans certains États membres. Ce seuil a été choisi pour garantir à tous les États membres l'équilibre entre efficacité des enquêtes judiciaires d'une part, et protection des droits et du principe de proportionnalité d'autre part. Un seuil offre aussi l'avantage d'être facilement applicable en pratique.

Les injonctions de production portant sur des données relatives aux transactions ou sur celles relatives au contenu peuvent aussi être émises pour des infractions harmonisées spécifiques décrites dans la disposition et pour lesquelles les preuves ne sont généralement disponibles qu'en format électronique. L'application du règlement se justifie aussi lorsque la peine privative de liberté maximale est inférieure au seuil ci-dessus; autrement, les enquêtes judiciaires liées à ces infractions pourraient ne pas être menées correctement et entraîner l'impunité des auteurs. Les infractions font l'objet des dispositions spécifiques suivantes: i) décision-cadre 2001/413/JAI du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, ii) la directive 2011/93UE 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, et iii) la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil. Les injonctions peuvent aussi être émises pour les infractions décrites dans la directive 2017/541/UE 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. Certaines de ces infractions sont assorties d'un seuil minimal de peine maximale d'au moins un an, d'autres de deux ans, mais aucun seuil minimal n'est inférieur à un an.

L'article définit aussi les informations obligatoires devant figurer sur l'injonction européenne de production afin que le fournisseur de services puisse identifier et produire les données requises. L'injonction européenne de production inclut également le raisonnement motivé sur la nécessité et la proportionnalité de cette mesure.

L'injonction est mise en œuvre par l'intermédiaire d'un certificat d'injonction européenne de production (EPOC) (voir l'article 8), envoyé après traduction au fournisseur de services. L'EPOC contient les mêmes informations obligatoires que l'injonction, à l'exception des motifs appuyant la nécessité et la proportionnalité de la mesure ou de détails supplémentaires sur l'affaire.

Lorsque les données requises sont stockées ou traitées à travers une infrastructure mise à la disposition d'une entreprise par un fournisseur de services, généralement dans le cas des services d'hébergement ou logiciels, ladite entreprise est considérée comme le destinataire de la demande émise par les autorités chargées de l'enquête. Une procédure de décision d'enquête européenne ou d'entraide judiciaire s'avère alors nécessaire si l'entreprise n'est pas un fournisseur de services couvert par le champ d'application du présent règlement. Le fournisseur de services n'est le destinataire d'une injonction européenne de production que lorsqu'il est inapproprié qu'une entreprise tienne ce rôle, en particulier s'il y a un risque de compromettre l'enquête, par exemple si l'entreprise elle-même fait l'objet de l'enquête.

Avant d'émettre une injonction européenne de production, l'autorité d'émission doit tenir compte également des immunités et des privilèges éventuels prévus par les lois de l'État membre du fournisseur de services, ou des éventuelles conséquences sur les intérêts fondamentaux de cet État membre tels que la sécurité nationale et la défense. Cette disposition vise à garantir la prise en considération, par l'État d'émission des immunités et des privilèges protégeant les données requises dans l'État membre du fournisseur de services, en particulier lorsqu'ils assurent une protection plus élevée que la législation de l'État d'émission.

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

Une injonction européenne de conservation est soumise à des conditions similaires à celles de l'injonction de production. Elle peut être émise pour toute infraction répondant aux autres conditions fixées à l'article 6. Elle vise également à empêcher le retrait, la suppression ou la modification des données concernées lorsque leur production risque de prendre plus de temps, par exemple en raison de l'utilisation de canaux de coopération judiciaire. Par exemple, vu que la décision d'enquête européenne peut généralement valoir pour toute infraction sans distinction de seuil, il en va de même pour l'injonction européenne de conservation. Autrement, cet instrument ne serait pas efficace. Les injonctions européennes de conservation peuvent aussi être émises ou validées par un procureur afin de permettre aux autorités chargées des enquêtes d'agir rapidement, pourvu que ces injonctions soient suivies d'une demande appropriée de production de données et dont toutes les conditions feront l'objet d'un nouvel examen.

Article 7: Destinataire d'une injonction européenne de production ou d'une injonction européenne de conservation

Les injonctions européennes de production et de conservation devraient être adressées à un représentant légal désigné par le fournisseur de services aux fins de recueillir des preuves dans le cadre de procédures pénales, conformément à la directive établissant les règles harmonisées de désignation des représentants légaux aux fins de recueillir des preuves dans le cadre de procédures pénales. La transmission se fera sous la forme d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR) visés à l'article 8. Ce représentant légal sera chargé de la réception de ces certificats, et devra les exécuter pleinement en temps voulu. Les fournisseurs de services ont ainsi le choix quant à la façon de s'organiser pour produire les données requises par les autorités de l'État membre.

Si aucun représentant légal n'a été désigné, les injonctions peuvent alors être adressées à l'établissement du fournisseur de services sur le territoire de l'Union. Cette solution de repli garantit l'efficacité du système si le fournisseur de services n'a pas (encore) désigné de représentant légal, par exemple en l'absence d'une telle obligation au titre de la directive, si le fournisseur de services est établi et actif uniquement dans un État membre ou si aucune obligation de désigner un représentant n'est encore entrée en vigueur avant le délai de transposition de la directive.

En cas de manquement de la part du représentant légal, deux situations permettent à l'autorité d'émission d'adresser l'injonction à tout établissement du fournisseur situé dans l'Union: dans les cas d'urgence au sens de l'article 9, paragraphe 2, et dans les cas où le représentant légal ne respecte pas ses obligations au titre des articles 9 et 10, si l'autorité d'émission estime qu'il existe un risque clair de perte des données.

Article 8: Certificat d'injonction européenne de production et certificat d'injonction européenne de conservation

L'EPOC et l'EPOC-PR servent à transmettre les injonctions au destinataire visé à l'article 7. Les modèles pour les deux certificats sont fournis aux annexes I et II du règlement; ils doivent être traduits dans l'une des langues officielles de l'État membre où se trouve le destinataire. Le fournisseur de services peut confirmer que les versions des injonctions dans d'autres langues officielles de l'Union seront aussi acceptées. Ces certificats visent à fournir toutes les

informations nécessaires à transmettre au destinataire dans un format standard qui réduit les sources d'erreur, permet d'identifier facilement les données et évite au maximum le texte libre, diminuant ainsi les coûts de traduction. Pour éviter de compromettre les enquêtes, le certificat n'inclut pas le plein raisonnement sur la base des motifs appuyant la nécessité et la proportionnalité ni d'autres détails sur l'affaire. Le certificat ne sert donc que comme complément à l'injonction elle-même afin de permettre au suspect de la contester ultérieurement pendant la procédure pénale.

Certains fournisseurs de services ont déjà mis en place des plateformes pour permettre aux services répressifs de soumettre leurs demandes. Le règlement ne devrait pas empêcher l'utilisation de telles plateformes étant donné qu'elles présentent de nombreux avantages, notamment la possibilité d'une authentification facile et une transmission sécurisée des données. Cependant, ces plateformes doivent autoriser la soumission des EPOC et EPOC-PR dans le format défini aux annexes I et II, sans demander d'autres informations liées à l'injonction.

Les plateformes créées par les États membres ou les organismes de l'Union peuvent aussi procurer des moyens de transmission sécurisés et faciliter l'authentification des injonctions et la collecte de statistiques. Il conviendrait d'envisager l'élargissement éventuel des plateformes eCodes et SIRIUS afin de mettre en place une connexion sécurisée avec les fournisseurs de services pour la transmission des EPOC et EPOC-PR ainsi que la réponse des fournisseurs, le cas échéant.

Article 9: Exécution d'un EPOC

L'article 9 contraint le destinataire à répondre aux EPOC et indique les délais obligatoires. Le délai normal est de dix jours, mais les autorités peuvent fixer un délai plus court si cela est justifié. En outre, dans les cas d'urgence, définis comme une situation présentant une menace imminente pour la vie ou l'intégrité physique d'une personne ou pour une infrastructure essentielle, le délai est réduit à 6 heures.

La disposition garantit aussi la possibilité d'un dialogue entre le destinataire et l'autorité d'émission. Si l'EPOC est incomplet, manifestement incorrect ou dépourvu des informations suffisantes au fournisseur de services pour l'exécution dudit EPOC, le destinataire contacte l'autorité d'émission pour obtenir des clarifications à l'aide du formulaire fourni à l'annexe III. Il signale également à l'autorité d'émission son incapacité à fournir les données en raison d'un cas de force majeure ou d'impossibilité de fait. Tel est notamment le cas si la personne dont les données sont requises n'était pas client de ce service ou — par exemple au titre d'autres obligations de confidentialité — si lesdites données ont été illégalement supprimées par le fournisseur de services avant réception de l'injonction par son ou ses représentants légaux. L'autorité d'émission devrait être informée de ces circonstances pour réagir rapidement, pour recueillir éventuellement les preuves électroniques auprès d'un autre fournisseur de services, et pour éviter que l'autorité d'émission ne lance une procédure d'exécution dépourvue de sens.

Si le destinataire ne fournit pas du tout les informations, ou pas de façon complète ni opportune, pour d'autres raisons que celles précitées, il doit communiquer ces raisons à l'autorité d'émission à l'aide du formulaire fourni à l'annexe III. Le destinataire peut alors s'adresser à l'autorité d'émission pour résoudre tout problème lié à l'exécution de l'EPOC. L'autorité d'émission peut ainsi rectifier ou réexaminer l'EPOC à un stade précoce avant la phase d'exécution.

Si les données ne sont pas produites immédiatement, notamment en cas de dialogue lancé entre le destinataire et l'autorité d'émission impliquant que les délais visés à l'article 9, paragraphe 1, ne pourront être respectés, le fournisseur de service a l'obligation de conserver les données afin de ne pas les perdre dès réception de l'EPOC, pourvu que lesdites données puissent être identifiées. La conservation peut être requise par voie de l'EPOC détaillé ou d'une demande ultérieure d'entraide judiciaire ou de décision d'enquête européenne remplaçant l'EPOC original.

Article 10: Exécution d'un EPOC-PR

L'exécution d'un EPOC-PR requiert de conserver les données disponibles au moment de la réception de l'injonction. Les fournisseurs de services devraient conserver les données aussi longtemps que nécessaire pour pouvoir les produire sur demande, à condition que l'autorité d'émission confirme dans un délai de soixante jours à compter de l'émission de l'injonction qu'elle a introduit la demande de production. Pour ce faire, certaines étapes réglementaires sont requises, notamment l'envoi d'une demande d'entraide judiciaire pour traduction.

Toutefois, les demandes de conservation ne devraient être émises ou maintenues que le temps nécessaire à l'introduction d'une demande ultérieure de production des données concernées. Pour éviter de conserver des données inutilement ou trop longtemps, l'autorité émettrice de l'injonction européenne de conservation informe le destinataire dès qu'une décision est prise de ne pas émettre ou de retirer une injonction de production ou une demande de coopération judiciaire.

Cette disposition, similaire à celles de l'article 9, garantit aussi la possibilité d'un dialogue entre le destinataire et l'autorité d'émission. Si l'EPOC-PR est incomplet, manifestement incorrect ou dépourvu des informations suffisantes pour que le fournisseur de services puisse exécuter ledit EPOC-PR, le destinataire contacte l'autorité d'émission pour obtenir des clarifications à l'aide du formulaire fourni à l'annexe III. Il signale également à l'autorité d'émission lorsqu'il est dans l'incapacité de fournir les données en raison de circonstances considérées comme un cas de force majeure ou une impossibilité de fait, ou pour d'autres raisons.

Article 11: Confidentialité et information de l'utilisateur

Il convient de protéger la confidentialité de l'enquête en cours, notamment l'existence de toute injonction émise pour obtenir des données pertinentes. Cet article s'inspire de l'article 19 de la directive relative à la décision d'enquête européenne. D'une part, il prévoit l'obligation pour le destinataire, ou le fournisseur de services, dans le cas où ils sont différents, de préserver la confidentialité de l'EPOC ou l'EPOC-PR, notamment en s'abstenant d'informer la personne dont les données sont requises lorsque l'autorité d'émission l'exige afin de protéger l'enquête judiciaire, conformément à l'article 23 du RGPD.

D'autre part, il est important que la personne dont les données sont requises soit informée, notamment pour l'exercice des recours légaux. Si le fournisseur de services ne s'en charge pas, à la demande de l'autorité d'émission, celle-ci informe alors la personne conformément à l'article 13 de la directive en matière de protection des données dans le domaine répressif dès qu'il n'existe plus de risque de compromettre l'enquête, et lui fournit les informations requises concernant les recours légaux. Ces informations interférant moins avec les droits

concernés, elles ne sont pas fournies dans le cas d'une injonction européenne de conservation; elles le sont uniquement pour les injonctions européennes de production.

Article 12: Remboursement des frais

Si le droit national de l'État d'émission le prévoit pour les injonctions nationales dans des affaires nationales similaires, les fournisseurs de services peuvent aussi réclamer le remboursement de leurs frais auprès de l'État d'émission conformément au droit national de celui-ci. Cette disposition garantit le traitement équitable des fournisseurs de services destinataires d'une injonction nationale et d'un EPOC du même État membre, dans le cas où cet État membre a choisi de rembourser certains fournisseurs de services. Cependant, la proposition de règlement n'harmonise pas le remboursement des frais étant donné que les différents États membres ont posé des choix différents cet égard.

Les frais peuvent être réclamés directement par le fournisseur de services ou par l'intermédiaire de son représentant légal. Ces frais ne peuvent être remboursés qu'une seule fois.

Chapitre 3: Sanctions et mise en œuvre

Article 13: Sanctions

Les États membres veillent à la mise en place de sanctions pécuniaires efficaces, proportionnées et dissuasives pour les fournisseurs de services qui ne respectent pas leurs obligations au titre des articles 9, 10 et 11. Cela s'applique sans préjudice des lois nationales qui prévoient des sanctions pénales pour de telles situations.

Article 14: Procédure de mise en œuvre

L'article 14 prévoit une procédure de mise en œuvre des injonctions en cas de non-respect, avec l'assistance de l'État membre où est établi le destinataire du certificat. Selon le destinataire initial, il s'agit soit de l'État membre du fournisseur de services, soit celui du représentant légal. L'autorité d'émission transfère l'injonction complète y compris le raisonnement relatif à sa nécessité et à sa proportionnalité, accompagnée du certificat, à l'autorité compétente dans l'État chargé de la mise en œuvre qui veille à sa mise en œuvre conformément à sa législation nationale en recourant, si nécessaire, aux sanctions visées à l'article 13. Si l'injonction est renvoyée pour application à l'État chargé de la mise en œuvre, l'autorité chargée de la mise en œuvre peut décider de ne pas reconnaître ou de ne pas mettre en œuvre l'injonction si elle considère, au moment de sa réception, que l'un des motifs limités de refus s'applique, et après consultation de l'autorité d'émission. En outre, si la procédure de mise en œuvre est tout de même lancée, le destinataire peut lui-même s'opposer à l'injonction devant l'autorité chargée de la mise en œuvre. Il peut y procéder sur la base des motifs avancés, à l'exception des immunités et privilèges mais y compris dans les cas où l'injonction n'a manifestement pas été émise ou validée par une autorité compétente, ou si le respect de l'injonction constitue une violation manifeste de la Charte des droits fondamentaux de l'Union européenne ou s'avère abusif. Par exemple, une injonction demandant la production de données relatives au contenu appartenant à une classe indéfinie d'individus dans une zone géographique ou sans lien avec une procédure pénale réelle ignorerait de façon évidente les conditions d'émission d'une injonction européenne de production fixées dans le présent règlement, et cela ressortirait clairement du certificat lui-même. Seule la personne dont les données sont requises peut invoquer d'autres motifs dans le cadre des recours légaux propres à l'État d'émission (voir article 17 ci-dessous). En outre, les fournisseurs de services

disposent d'un recours légal contre la décision de l'autorité chargée de la mise en œuvre de leur infliger une sanction.

La procédure de mise en œuvre prévoit plusieurs délais pour les autorités d'émission et les autorités chargées de la mise en œuvre afin d'éviter tout retard supplémentaire au cours de la procédure.

Chapitre 4: Recours

Articles 15 et 16: Procédure de réexamen en cas d'obligations contradictoires découlant des lois d'un pays tiers

Les articles 15 et 16 prévoient une procédure de réexamen dans le cas des fournisseurs de services établis dans des pays tiers et qui font face à des obligations contradictoires. Ces dispositions sont également cruciales pour garantir la protection des droits individuels et de la courtoisie internationale. En fixant des normes strictes, elles aspirent à encourager les pays tiers à mettre en place un niveau de protection similaire. Dans la situation inverse, lorsque les autorités d'un pays tiers cherchent à obtenir les données d'un citoyen européen auprès d'un fournisseur de services de l'UE, la législation de l'Union ou des États membres relative à la protection des droits fondamentaux, comme l'acquis en matière de protection des données, permettent d'empêcher de la même façon la divulgation de ces données. L'Union européenne attend des pays tiers qu'ils respectent ces interdictions tout comme le fait la présente proposition.

La procédure visée à l'article 15 peut être déclenchée par le destinataire si le respect de l'injonction européenne de production entraînait une violation d'une ou plusieurs lois d'un pays tiers interdisant la divulgation de données au nom de la nécessité de protéger les droits fondamentaux des individus concernés ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales. Le destinataire est tenu d'informer l'autorité d'émission par voie d'une opposition motivée des fondements de sa conclusion qu'il existe des obligations contradictoires. Cette opposition motivée ne peut se baser sur le simple fait que des dispositions similaires ne sont pas prévues par le droit du pays tiers ni sur la seule circonstance du stockage des données dans un pays tiers. L'opposition motivée est soulevée conformément à la procédure visée à l'article 9, paragraphe 5, pour notifier l'intention de ne pas se conformer aux obligations dont il est question à l'aide du formulaire fourni à l'annexe III.

L'autorité d'émission examine sa propre injonction à la lumière de cette opposition motivée. Si elle choisit de retirer l'injonction, la procédure prend fin. Si elle choisit de maintenir l'injonction, l'affaire est transférée à la juridiction compétente de son État membre. La juridiction examine alors, en se basant sur l'opposition motivée et en tenant compte de tous les faits pertinents pour l'affaire, si le droit du pays tiers s'applique au cas concerné en particulier — et si tel est le cas — s'il existe un conflit dans l'affaire en question. Pour procéder à cette évaluation, la juridiction doit évaluer si la législation du pays tiers, plutôt que d'être destinée à protéger les droits fondamentaux ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, vise manifestement à protéger d'autres intérêts ou vise à protéger des activités illégales de demandes d'application de la loi dans le contexte d'enquêtes criminelles

Si la juridiction confirme l'existence effective d'un conflit entre les obligations au titre de la législation protégeant les droits fondamentaux des individus ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales, il doit solliciter l'avis du pays tiers concerné par l'intermédiaire des autorités centrales nationales dudit pays. Si le pays tiers

consulté confirme l'existence du conflit et s'oppose à l'exécution de l'injonction, la juridiction doit alors retirer l'injonction.

Si le conflit naît d'une autre disposition législative de ce pays tiers qui ne vise pas à protéger les droits fondamentaux des individus ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales, la juridiction prend alors sa décision de manière à trouver un équilibre entre les intérêts favorables et défavorables d'un maintien de l'injonction.

Les conditions fixées à l'article 9, en particulier les obligations de conservation décrites à son paragraphe 6, sont également applicables aux situations d'obligations contradictoires découlant du droit d'un pays tiers. Si la juridiction décide de maintenir l'injonction, l'autorité d'émission et le fournisseur de services en sont informés en vue de procéder à son exécution. Si l'injonction est levée, une injonction de conservation séparée peut être émise afin d'assurer la disponibilité des données qui pourraient être obtenues par l'intermédiaire d'une demande d'entraide judiciaire.

Vu que l'injonction européenne de conservation n'entraîne pas en soi la divulgation des données et donc aucune inquiétude similaire, la procédure de réexamen se limite à l'injonction européenne de production.

Article 17: Recours effectifs

Cette disposition garantit des recours effectifs aux personnes concernées par une injonction européenne de production. Ces recours s'exercent dans l'État d'émission conformément à la législation nationale. Pour les suspects et les personnes poursuivies, les recours s'exercent normalement pendant la procédure pénale. Aucun recours n'existe pour l'injonction européenne de conservation, laquelle n'autorise en aucun cas la divulgation de données, excepté lorsqu'elle est suivie d'une injonction européenne de production ou d'un autre instrument conduisant à la divulgation des données, auquel cas des recours spécifiques sont prévus.

Les personnes dont les données sont requises alors qu'elles ne sont ni suspectées ni poursuivies dans le cadre de procédures pénales ont également droit à un recours légal dans l'État d'émission. Tous ces droits sont sans préjudice des éventuels recours prévus au titre de la directive en matière de protection des données dans le domaine répressif et du RGPD.

Contrairement aux dispositions prévues pour les fournisseurs de services, le règlement ne limite pas les motifs possibles que ces personnes peuvent avancer pour contester la légalité de l'injonction. Ces motifs englobent la nécessité et la proportionnalité de l'injonction.

L'exercice de recours dans l'État d'émission ne doit pas représenter une charge disproportionnée pour les personnes concernées. Comme pour les décisions exécutées au moyen d'autres formes de coopération judiciaire, les tribunaux de l'État d'émission sont les mieux placés pour examiner la légalité des injonctions européennes de production émises par leurs propres autorités et pour évaluer leur compatibilité avec leur propre législation nationale. De plus, lors de la phase de mise en œuvre, les destinataires peuvent s'opposer séparément à la mise en œuvre de l'EPOC ou de l'EPOC-PR dans leur État membre d'accueil sur la base d'une liste de motifs énumérés dans le règlement (voir l'article 14 ci-dessus).

Article 18: Garantie des privilèges et des immunités en vertu du droit de l'État de réception

Cette disposition poursuit le même objectif que celui de l'article 5, paragraphe 7, à savoir garantir la prise en considération par l'État d'émission des immunités et des privilèges qui

protègent les données requises dans l'État membre du fournisseur de services, notamment lorsque ces immunités et ces privilèges sont différents dans les deux États membres, ainsi que des intérêts fondamentaux de cet État membre en matière de sécurité et de défense nationales. L'article 18 prévoit que la juridiction de l'État d'émission en tient compte comme s'ils existaient au titre du droit national dudit État. En raison des différences entre les États membres au niveau de l'évaluation de la pertinence et de la recevabilité d'une preuve, la disposition accorde une certaine souplesse aux tribunaux concernant la manière de procéder.

Chapitre 5: Dispositions finales

Article 19: Suivi et rapports

Cet article impose aux États membres de communiquer les informations spécifiques liées à l'application du règlement en vue d'assister la Commission dans l'exercice de ses fonctions au titre de l'article 24. La Commission doit établir un programme détaillé de suivi des réalisations, des résultats et des incidences de ce règlement.

Article 20: Modification des certificats et des formulaires

Les certificats et formulaires figurant aux annexes I, II et III de la présente proposition faciliteront l'exécution d'un EPOC et d'un EPOC-PR. C'est la raison pour laquelle il est nécessaire d'avoir la possibilité d'améliorer éventuellement le contenu du certificat et du formulaire le plus rapidement possible dès que le besoin s'en fera sentir. Cette exigence ne couvre pas la modification des trois annexes par l'intermédiaire d'une procédure législative ordinaire, lesquelles ne constituent pas des éléments essentiels des actes législatifs, les principaux éléments étant définis à l'article 8. Par conséquent, l'article 20 définit une procédure plus rapide et plus souple pour procéder aux modifications par l'intermédiaire d'actes délégués.

Article 21: Exercice de la délégation

Cet article fixe les conditions en vertu desquelles la Commission a le pouvoir d'adopter des actes délégués pour apporter les modifications nécessaires au certificat et aux formulaires joints à la proposition. Il établit la procédure standard pour l'adoption de ces actes délégués.

Article 22: Notifications

Les États membres doivent signaler à la Commission qui sont les autorités d'émission et de mise en œuvre, et quels sont les tribunaux compétents pour traiter les oppositions motivées de fournisseurs de services en cas de conflit de lois.

Article 23: Rapport avec les décisions d'enquête européennes

Cette disposition précise que le règlement n'empêche pas les autorités de l'État membre d'émettre des décisions d'enquête européennes au titre de la directive 2014/41/UE pour obtenir des preuves électroniques.

Article 24: Évaluation

Cette disposition précise que la Commission procède à une évaluation du présent règlement conformément aux lignes directrices de la Commission pour une meilleure réglementation et en vertu du paragraphe 22 de l'accord interinstitutionnel du 13 avril 2016[25]. La Commission tiendra le Parlement européen et le Conseil informés des conclusions de l'évaluation, incluant une évaluation du besoin d'élargir le champ d'application aux services non encore couverts mais susceptibles d'avoir plus d'importance pour les enquêtes, cinq ans après l'entrée en vigueur du règlement proposé.

Article 25: Entrée en vigueur

Le règlement proposé entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel. Le règlement s'applique 6 mois après sa date d'entrée en vigueur.

[25] Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne «Mieux légiférer» du 13 avril 2016; JO L 123 du 12.5.2016, p. 1-14.

2018/0108 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière 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[26],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

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

(2) Les mesures visant à obtenir et à conserver des preuves électroniques sont de plus en plus importantes pour permettre des enquêtes et des poursuites pénales dans l'ensemble de l'Union. Des mécanismes efficaces pour obtenir des preuves électroniques sont essentiels pour lutter contre la criminalité, sous réserve de conditions garantissant le plein respect des droits et principes fondamentaux reconnus dans la charte des droits fondamentaux de l'Union européenne tels que consacrés dans les traités, et en particulier les principes de nécessité et de proportionnalité, de légalité, de protection des données, de secret de la correspondance et de protection de la vie privée.

(3) La déclaration conjointe des ministres de la justice et des affaires intérieures du 22 mars 2016 et des représentants des institutions de l'Union sur les attentats terroristes à Bruxelles a souligné la nécessité de trouver en priorité des moyens de recueillir et d'obtenir des preuves électroniques plus rapidement et plus efficacement et de définir des mesures concrètes pour s'attaquer à cette question.

(4) Les conclusions du Conseil du 9 juin 2016 ont souligné l'importance croissante des preuves électroniques dans les procédures pénales, et de protéger le cyberespace contre les abus et les activités criminelles au profit des économies et des sociétés, et

[26] JO C , , p. .

donc la nécessité pour les autorités répressives et judiciaires de disposer d'outils efficaces pour enquêter sur les actes délictueux commis en rapport avec le cyberespace et en poursuivre les auteurs.

(5) Dans la communication conjointe sur la résilience, la dissuasion et la défense du 13 septembre 2017[27], la Commission a souligné que l'efficacité des enquêtes et des poursuites relatives aux infractions facilitées par les technologies de l'information et de la communication constitue un moyen de dissuasion essentiel contre les cyberattaques, et que le cadre procédural actuel doit être mieux adapté à l'ère d'internet. Les procédures actuelles ne sont pas toujours suffisantes en raison de la rapidité des cyberattaques, qui créent un besoin particulier de coopération transfrontière rapide.

(6) Le Parlement européen a repris ces préoccupations dans sa résolution sur la lutte contre la cybercriminalité du 3 octobre 2017[28], en soulignant les défis que le cadre juridique actuellement fragmenté peut créer pour les fournisseurs de services cherchant à se conformer aux demandes des services répressifs, et en appelant la Commission à élaborer un cadre juridique pour les preuves électroniques offrant des garanties suffisantes pour les droits et les libertés de tous les intéressés.

(7) Les services basés sur un réseau peuvent être fournis à partir de n'importe quel endroit et ne nécessitent pas d'infrastructure physique, de locaux ou de personnel dans le pays concerné. En conséquence, les éléments de preuve pertinents sont souvent stockés hors de l'État menant l'enquête ou par un fournisseur de services établi en dehors de cet État. Il n'existe souvent pas d'autre lien entre l'affaire faisant l'objet de l'enquête dans l'État concerné et l'État du lieu de stockage ou de l'établissement principal du fournisseur de services.

(8) En raison de ce manque de lien, des demandes de coopération judiciaire sont souvent adressées à des États qui hébergent un grand nombre de fournisseurs de services, mais qui n'ont aucun autre rapport avec le cas en question. En outre, le nombre de demandes s'est multiplié en raison de l'utilisation croissante des services en réseau, qui sont transfrontières par nature. En conséquence, l'obtention de preuves électroniques par les canaux de coopération judiciaire prend souvent beaucoup de temps, un délai plus long que celui de la disponibilité des indices. Il n'existe par ailleurs pas de cadre clair pour la coopération avec les fournisseurs de services, tandis que certains fournisseurs de pays tiers acceptent des demandes directes de données non relatives au contenu, conformément à leur législation nationale applicable. En conséquence, tous les États membres s'appuient sur le canal de coopération avec les fournisseurs de services lorsqu'il existe, en utilisant différents outils nationaux et différentes conditions et procédures nationales. En outre, pour les données relatives au contenu, certains États membres ont pris des mesures unilatérales, tandis que d'autres continuent de s'appuyer sur la coopération judiciaire.

(9) La fragmentation du cadre juridique crée des défis pour les fournisseurs de services qui cherchent à se conformer aux demandes des services répressifs. Par conséquent, il est nécessaire de proposer un cadre juridique européen pour les preuves électroniques afin d'imposer aux fournisseurs de services couverts par le champ d'application de l'instrument l'obligation de répondre directement aux autorités sans l'intervention d'une autorité judiciaire dans l'État membre du fournisseur de services.

---

27 JOIN(2017) 450 final.

28 2017/2068(INI).

(10) Les injonctions au titre du présent règlement doivent être adressées aux représentants légaux des fournisseurs de services désignés à cet effet. Si un fournisseur de services établi dans l'Union n'a pas désigné de représentant légal, les injonctions peuvent être adressées à tout établissement de ce fournisseur de services dans l'Union. Cette option de repli sert à garantir l'efficacité du système si le fournisseur de services n'a pas (encore) désigné de représentant spécifique.

(11) Le mécanisme des injonctions européennes de production et de conservation de preuves électroniques en matière pénale ne peut fonctionner que sur la base d'un niveau élevé de confiance mutuelle entre les États membres, qui constitue une condition préalable essentielle au bon fonctionnement de cet instrument.

(12) Le présent règlement respecte les droits fondamentaux et observe les principes reconnus en particulier par la charte des droits fondamentaux de l'Union européenne. Ceux-ci comprennent le droit à la liberté et à la sécurité, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif et à un procès équitable, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité, ainsi que le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction. Si l'État membre d'émission dispose d'indications selon lesquelles une procédure pénale parallèle pourrait être en cours dans un autre État membre, il doit consulter les autorités de cet État membre conformément à la décision-cadre 2009/948/JAI du Conseil[29].

(13) Afin de garantir le plein respect des droits fondamentaux, le présent règlement se réfère explicitement aux normes nécessaires concernant l'obtention de toutes données à caractère personnel, le traitement de ces données, le contrôle juridictionnel du recours à la mesure d'enquête prévue par le présent instrument et les recours disponibles.

(14) Le présent règlement s'applique sans préjudice des droits procéduraux dans les procédures pénales énoncés dans les directives 2010/64/UE[30], 2012/13/UE[31], 2013/48/UE[32], 2016/343[33], 2016/800[34] et 2016/1919[35] du Parlement européen et du Conseil.

---

29 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).

30 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).

31 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).

32 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).

33 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).

34 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).

35 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

(15) Le présent instrument fixe les règles selon lesquelles une autorité judiciaire compétente de l'Union européenne peut ordonner à un fournisseur de services proposant des services dans l'Union de produire ou de conserver des preuves électroniques au moyen d'une injonction européenne de production ou de conservation. Le présent règlement s'applique dans tous les cas où le fournisseur de services est établi ou représenté dans un autre État membre. Dans le contexte national où les instruments prévus par le présent règlement ne peuvent être utilisés, le règlement ne doit pas limiter pas les pouvoirs des autorités nationales compétentes déjà prévus par la législation nationale pour contraindre les fournisseurs de services établis ou représentés sur leur territoire.

(16) Les fournisseurs de services les plus pertinents pour les procédures pénales sont les fournisseurs de services de communications électroniques et les fournisseurs spécifiques de services de la société de l'information qui facilitent les interactions entre les utilisateurs. Dès lors, ces deux groupes sont couverts par le présent règlement. Les fournisseurs de services de communications électroniques sont définis dans la proposition de directive établissant le code des communications électroniques européen. Ils comprennent les communications interpersonnelles telles que la voix par le protocole de l'internet, la messagerie instantanée et les services de courrier électronique. Les catégories de services de la société de l'information incluses ici sont celles pour lesquelles le stockage de données est une composante déterminante du service fourni à l'utilisateur, et concernent en particulier les réseaux sociaux dans la mesure où ils ne sont pas considérés comme des services de communication électronique, les places de marché en ligne facilitant les transactions entre leurs utilisateurs (tels que des consommateurs ou des entreprises) et les autres services d'hébergement, notamment lorsque le service est fourni par l'intermédiaire de l'informatique en nuage. Les services de la société de l'information pour lesquels le stockage des données ne constitue pas un élément déterminant du service fourni à l'utilisateur et pour lesquels il ne présente qu'un caractère accessoire, tels que les services juridiques ou les services d'architecture, d'ingénierie et de comptabilité fournis à distance en ligne, doivent être exclus du champ d'application du présent règlement, même s'ils sont susceptibles de relever de la définition des services de la société de l'information conformément à la directive (UE) 2015/1535.

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

(18) Les fournisseurs de services d'infrastructure internet liés à l'attribution de noms et de numéros, tels que les bureaux d'enregistrement et les registres de noms de domaine et les fournisseurs de services d'anonymisation et d'enregistrement fiduciaire, ou les registres internet régionaux pour les adresses de protocole de l'internet («IP»), sont particulièrement pertinents lorsqu'il s'agit d'identifier des acteurs cachés derrière des sites internet malveillants ou compromis. Ils détiennent des données particulièrement

---

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).

pertinentes pour les procédures pénales, qui permettent d'identifier une personne ou une entité cachée derrière un site internet utilisé dans une activité criminelle, ou la victime d'une activité criminelle si un site internet compromis a été détourné par des criminels.

(19) Le présent règlement régule la collecte des données stockées uniquement, c'est-à-dire des données détenues par un fournisseur de services au moment de la réception d'un certificat d'injonction européenne de production ou de conservation. Il ne prévoit pas d'obligation générale de conservation des données, et n'autorise pas l'interception de données ou l'obtention de données stockées à un moment ultérieur à la réception d'un certificat d'injonction de production ou de conservation. Les données doivent être fournies, qu'elles soient cryptées ou non.

(20) Les catégories de données couvertes par le présent règlement comprennent les données relatives aux abonnés, les données relatives à l'accès et les données relatives aux transactions (ces trois catégories étant désignées comme les «données non relatives au contenu») et les données relatives au contenu. Cette distinction, sauf pour les données relatives à l'accès, existe dans le droit de nombreux États membres, ainsi que dans le cadre juridique actuel des États-Unis, qui permet aux fournisseurs de services de partager les données non relatives au contenu avec les autorités répressives étrangères sur une base volontaire.

(21) Il y a donc lieu de distinguer les données relatives à l'accès comme une catégorie de données spécifique utilisée dans le présent règlement. Les données relatives à l'accès sont demandées pour le même objectif que les données relatives aux abonnés, à savoir pour identifier l'utilisateur sous-jacent, et le niveau d'interférence avec les droits fondamentaux est similaire à celui des données relatives aux abonnés. Les données relatives à l'accès sont généralement enregistrées dans le cadre d'un enregistrement d'événements (un journal de serveur) pour indiquer le début et la fin d'une session d'accès d'un utilisateur à un service. Il s'agit souvent d'une adresse IP individuelle (statique ou dynamique) ou d'un autre identifiant qui indique l'interface réseau utilisée lors de la session d'accès. Si l'utilisateur est inconnu, il est souvent nécessaire de l'identifier avant que les données relatives aux abonnés liées à cet identifiant puissent être demandées au fournisseur de services.

(22) D'autre part, les données relatives aux transactions sont généralement demandées pour obtenir des informations sur les contacts de l'utilisateur et le lieu où il se trouve, et peuvent servir à établir le profil d'une personne concernée. Cela dit, les données relatives à l'accès seules ne peuvent pas servir à atteindre un objectif similaire; car elles ne révèlent par exemple aucune information sur les interlocuteurs de l'utilisateur. Dès lors, la présente proposition introduit une nouvelle catégorie de données, qui doivent être traitées comme des données relatives aux abonnés si l'objectif de la demande d'obtention de ces données est similaire.

(23) Toutes les catégories de données contiennent des données à caractère personnel et sont par conséquent couvertes par les garanties prévues par l'acquis de l'Union en matière de protection des données, mais l'intensité de l'incidence sur les droits fondamentaux varie, en particulier entre les données relatives aux abonnés et les données relatives à l'accès d'une part et les données relatives aux transaction et les données relatives au contenu d'autre part. Alors que les données relatives aux abonnés et les données relatives à l'accès sont utiles pour obtenir de premiers indices dans une enquête sur l'identité d'un suspect, les données relatives aux transactions et les données relatives au contenu sont les plus pertinentes en tant que matériel probant. Il est donc essentiel

que toutes ces catégories de données soient couvertes par l'instrument. En raison du degré d'interférence différent avec les droits fondamentaux, des conditions différentes sont imposées pour obtenir des données relatives aux abonnés et des données relatives à l'accès d'une part, et des données relatives aux transactions et des données relatives au contenu d'autre part.

(24) L'injonction européenne de production et l'injonction européenne de conservation sont des mesures d'enquête qui ne doivent être prises que dans le cadre de procédures pénales spécifiques contre les auteurs connus ou encore inconnus d'une infraction pénale concrète qui a déjà été commise, après une évaluation individuelle de la proportionnalité et de la nécessité dans chaque cas.

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

(26) Le présent règlement s'applique aux fournisseurs de services qui proposent des services dans l'Union, et les injonctions prévues par le présent règlement ne peuvent être émises que pour les données relatives aux services offerts dans l'Union. Les services fournis exclusivement en dehors de l'Union n'entrent pas dans le champ d'application du présent règlement, même si le fournisseur de services est établi dans l'Union.

(27) Pour déterminer si un fournisseur de services fournit des services dans l'Union, il est nécessaire d'évaluer si le fournisseur de services permet à des personnes morales ou physiques d'un ou plusieurs États membres d'utiliser ses services. Toutefois, la seule accessibilité d'une interface en ligne, comme par exemple l'accessibilité du site internet du fournisseur de services, d'un intermédiaire ou d'une adresse électronique et d'autres coordonnées dans un ou plusieurs États membres prises isolément ne constituent pas une condition suffisante pour l'application du présent règlement.

(28) Un lien substantiel avec l'Union doit également être pertinent pour déterminer le champ d'application du présent règlement. Un tel lien substantiel avec l'Union doit être considéré comme existant lorsque le fournisseur de services possède un établissement dans l'Union. En l'absence d'un tel établissement, le critère de lien substantiel doit être évalué sur la base de l'existence d'un nombre significatif d'utilisateurs dans un ou plusieurs États membres, ou du ciblage des activités sur un ou plusieurs États membres. Le ciblage des activités vers un ou plusieurs États membres peut être déterminé sur la base de toutes les circonstances pertinentes, et notamment de facteurs comme l'utilisation d'une langue ou d'une monnaie généralement utilisées dans cet État membre ou ces États membres, ou la possibilité de commander des biens ou des services. Le ciblage des activités vers un État membre peut également être constaté sur la base de la disponibilité d'une application dans la boutique d'applications nationale correspondante, de la mise à disposition de publicité locale ou de publicité dans la langue utilisée dans cet État membre ou de la gestion des relations avec la clientèle, si un service après-vente est par exemple fourni dans la langue généralement utilisée dans cet État membre. Un lien substantiel doit également être constaté lorsqu'un fournisseur de services oriente ses activités vers un ou plusieurs États membres comme énoncé à l'article 17, paragraphe l, point c), du règlement 1215/2012 relatif à la compétence, à la reconnaissance et à l'exécution des

décisions en matière civile et commerciale[36]. En revanche, la fourniture du service en vue du seul respect de l'interdiction de discrimination prévue par le règlement (UE) 2018/302[37] ne peut être considérée, pour ce seul motif, comme orientant ou ciblant des activités vers un territoire donné au sein de l'Union.

(29) Une injonction européenne de production ne doit être émise que si elle s'avère nécessaire et proportionnée. L'évaluation doit tenir compte du fait que l'injonction est limitée à ce qui est nécessaire pour atteindre l'objectif légitime d'obtenir les données pertinentes et nécessaires pour servir de preuve uniquement dans le cas d'espèce.

(30) Lorsqu'une injonction européenne de production ou de conservation est émise, une autorité judiciaire doit toujours être incluse dans le processus de délivrance ou de validation de l'injonction. Compte tenu du caractère plus sensible des données relatives aux transactions et des données relatives au contenu, l'émission ou la validation des injonctions européennes de production pour ces catégories nécessite le réexamen d'un juge. Les données relatives aux abonnés et à l'accès étant moins sensibles, les injonctions européennes de production pour leur divulgation peuvent également être émises ou validées par des procureurs compétents.

(31) Pour la même raison, une distinction doit être faite en ce qui concerne le champ d'application matériel du présent règlement: les injonctions de production de données relatives aux abonnés et de données relatives à l'accès peuvent être émises pour toute infraction pénale, tandis que l'accès aux données relatives aux transactions et aux données relatives au contenu doit être soumis à des exigences plus strictes, pour refléter la nature plus sensible de ces données. Un seuil permet une approche plus proportionnée, en combinaison avec à un certain nombre d'autres conditions et garanties ex ante et ex post prévues dans la proposition pour assurer le respect de la proportionnalité et des droits des personnes concernées. En même temps, un seuil ne devrait pas limiter l'efficacité de l'instrument ni son utilisation par les praticiens. Autoriser la délivrance de décisions d'enquêtes pour des infractions assorties d'une peine d'emprisonnement d'une durée maximale d'au moins trois ans limite le champ d'application de l'instrument à des délits plus graves, sans affecter de façon excessive ses possibilités d'utilisation par les praticiens. Cela exclut du champ d'application un nombre significatif de délits considérés comme moins graves par les États membres, qui donnent lieu à une peine maximale plus courte. Cela offre également l'avantage d'être plus facile à appliquer dans la pratique.

(32) Il existe des infractions spécifiques pour lesquelles les preuves sont généralement disponibles exclusivement sous forme électronique, par nature particulièrement éphémère. C'est le cas des infractions relevant de la cybercriminalité, même celles qui ne sont pas forcément considérées comme graves en tant que telles mais qui peuvent causer des préjudices graves ou considérables, en particulier dans le cas où le préjudice individuel est faible mais touche globalement un grand nombre de victimes. Dans la plupart des cas où l'infraction a été commise au moyen d'un système d'information, l'application du même seuil que pour d'autres types d'infractions

---

36 Règlement (UE) 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).

37 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) nº 2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE (JO L 601 du 2.3.2018, p. 1).

conduirait généralement à l'impunité. Cela justifie que le règlement s'applique également aux infractions pour lesquelles la sanction est inférieure à trois ans d'emprisonnement. Les infractions supplémentaires liées au terrorisme telles que décrites dans la directive 2017/541/UE ne requièrent pas de seuil relatif à une durée maximale d'emprisonnement d'au moins trois ans.

(33) En outre, il est nécessaire de prévoir que l'injonction européenne de production ne peut être émise que si une mesure similaire est disponible pour la même infraction dans une situation nationale comparable dans l'État d'émission.

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

(35) Les immunités et les privilèges, qui peuvent concerner des catégories de personnes (comme les diplomates) ou des relations spécifiquement protégées (comme le secret professionnel), sont mentionnés dans d'autres instruments de reconnaissance mutuelle comme la décision d'enquête européenne. Leur portée et leur incidence diffèrent selon la législation nationale applicable qui doit être prise en considération au moment de l'émission de l'injonction, étant donné que l'autorité d'émission ne peut émettre l'injonction que si une injonction similaire est disponible dans une situation nationale comparable. En plus de ce principe de base, les immunités et privilèges protégeant les données relatives à l'accès, les données relatives aux transactions ou les données relatives au contenu dans l'État membre du fournisseur de services doivent être pris en considération dans la mesure du possible dans l'État d'émission de la même manière que s'ils étaient prévus dans la législation nationale de l'État d'émission. Ceci est particulièrement pertinent si la législation de l'État membre du fournisseur de services ou de son représentant légal destinataire prévoit une protection plus élevée que la législation de l'État d'émission. La disposition garantit également le respect des cas où la divulgation des données peut porter atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales. Afin d'offrir une garantie supplémentaire, ces aspects doivent être pris en considération non seulement lors de l'émission de l'injonction, mais également plus tard, lors de l'évaluation de la pertinence et de la recevabilité des données concernées au stade pertinent de la procédure pénale, et si une procédure d'exécution est engagée par l'autorité d'exécution.

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

(37) Les injonctions européennes de production et de conservation doivent être adressées au représentant légal désigné par le fournisseur de services. En l'absence de représentant légal désigné, les injonctions peuvent être adressées à un établissement du fournisseur de services dans l'Union. Cela peut être le cas lorsque le fournisseur de services n'a aucune obligation juridique de désigner un représentant légal. En cas de non-conformité par le représentant légal dans des situations d'urgence, l'injonction européenne de production ou de conservation peut également être adressée au fournisseur de services en complément ou en remplacement de la demande d'exécution de la décision initiale conformément à l'article 14. En cas de non-conformité par le représentant légal dans des situations non urgentes, mais en cas de risques évidents de perte de données, une injonction européenne de production ou de conservation peut également être adressée à tout établissement du fournisseur de services dans l'Union. En raison de ces différents scénarios possibles, le terme général de «destinataire» est utilisé dans les dispositions. Lorsqu'une obligation telle que la confidentialité s'applique non seulement au destinataire, mais également au fournisseur de services s'il n'est pas le destinataire, cela est précisé dans la disposition correspondante.

(38) Les injonctions européennes de production et de conservation doivent être transmises au fournisseur de services au moyen d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR), qui doit être traduit. Les certificats doivent contenir les mêmes informations obligatoires que les injonctions, à l'exception des motifs de la nécessité et de la proportionnalité de la mesure ou des détails supplémentaires concernant l'affaire, afin de ne pas compromettre les enquêtes. Cependant, comme ils font partie de l'injonction elle-même, ils permettent au suspect de la contester ultérieurement au cours de la procédure pénale. Le cas échéant, le certificat doit être traduit dans la ou les langues officielles, ou dans l'une des langues officielles de l'État membre du destinataire, ou dans une autre langue officielle explicitement acceptée par le fournisseur de services.

(39) L'autorité d'émission compétente doit transmettre l'EPOC ou l'EPOC-PR directement au destinataire par tout moyen à même de produire un document écrit dans des conditions permettant au fournisseur d'en établir l'authenticité, tel qu'un courrier recommandé, un courrier électronique ou des plateformes sécurisés ou d'autres canaux sécurisés, notamment ceux mis à disposition par le fournisseur de services, conformément aux règles protégeant les données à caractère personnel.

(40) Les données demandées doivent être transmises aux autorités au plus tard dans les 10 jours suivant la réception de l'EPOC. Des délais plus courts doivent être respectés par le fournisseur dans les cas d'urgence et si l'autorité d'émission indique d'autres raisons de s'écarter du délai de 10 jours. Outre le danger imminent de la suppression des données demandées, de telles raisons pourraient inclure des circonstances liées à une enquête en cours, par exemple lorsque les données demandées sont associées à d'autres mesures d'enquête urgentes qui ne peuvent être menées sans les données manquantes ou qui en dépendent.

(41) Afin de permettre aux fournisseurs de services de résoudre les problèmes formels, il est nécessaire de définir une procédure pour la communication entre le fournisseur de services et l'autorité judiciaire d'émission dans les cas où l'EPOC serait incomplet ou contiendrait des erreurs manifestes ou des informations insuffisantes pour l'exécution de l'injonction. Par ailleurs, si le fournisseur de services ne fournit pas les informations de manière exhaustive ou en temps opportun pour toute autre raison, par exemple parce qu'il pense qu'il existe un conflit vis à vis d'une obligation soumise à la loi d'un pays tiers, ou que l'injonction européenne de production n'a pas été émise en conformité avec les conditions prévues par le présent règlement, il doit en aviser les autorités d'émission et fournir les justifications appropriées. La procédure de communication doit donc largement permettre la correction ou le réexamen de l'EPOC par l'autorité d'émission à un stade précoce. Pour garantir la disponibilité des données, le fournisseur de services doit conserver les données s'il peut identifier les données demandées.

(42) Lorsqu'il reçoit un certificat d'injonction européenne de conservation (EPOC-PR), le fournisseur de services doit conserver les données demandées pendant 60 jours au maximum, sauf si l'autorité d'émission informe le fournisseur de services qu'elle a lancé la procédure pour l'émission d'une demande de production ultérieure, auquel cas la conservation doit être poursuivie. La période de 60 jours est calculée pour permettre l'introduction d'une demande officielle. De ce fait, quelques mesures formelles au moins doivent avoir été prises, par exemple, l'envoi d'une demande d'entraide judiciaire pour la traduction. Après réception de ces informations, les données doivent être conservées aussi longtemps que nécessaire jusqu'à ce qu'elles soient produites dans le cadre d'une demande ultérieure de production.

(43) Les fournisseurs de services et leurs représentants légaux doivent garantir la confidentialité et, si l'autorité d'émission le demande, s'abstenir d'informer la personne dont les données sont demandées afin de protéger l'enquête sur les infractions pénales, conformément à l'article 23 du règlement (UE) 2016/679[38]. Cependant, l'information de l'utilisateur constitue un élément essentiel pour permettre le contrôle juridictionnel et le recours juridictionnel, et elle doit être fournie par l'autorité s'il a été demandé au fournisseur de services de ne pas informer l'utilisateur, lorsqu'il n'y a aucun risque de compromettre les enquêtes en cours, conformément à la mesure nationale de mise en œuvre de l'article 13 de la directive (UE) 2016/680[39].

(44) En cas de non-conformité par le destinataire, l'autorité d'émission peut transférer l'injonction complète, notamment le raisonnement sur la nécessité et la proportionnalité, accompagnée du certificat, à l'autorité compétente de l'État membre où le destinataire du certificat réside ou est établi. Cet État membre doit l'exécuter en conformité avec la législation nationale. Les États membres doivent prévoir l'imposition de sanctions pécuniaires efficaces, proportionnées et dissuasives en cas de violation des obligations établies par le présent règlement.

---

38 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).

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

(45) La procédure d'exécution est une procédure par laquelle le destinataire peut s'opposer à l'exécution sur la base de certains motifs restreints. L'autorité d'exécution peut refuser de reconnaître et d'exécuter l'injonction basée sur les mêmes motifs, si les immunités et privilèges prévus par sa législation nationale s'appliquent ou si la divulgation risque de porter atteinte à ses intérêts fondamentaux tels que la sécurité et la défense nationales. L'autorité d'exécution doit consulter l'autorité d'émission avant de refuser de reconnaître ou d'exécuter l'injonction sur la base de ces motifs. En cas de non-conformité, les autorités peuvent imposer des sanctions. Ces sanctions doivent être proportionnées compte tenu également des circonstances spécifiques telles que les non-conformités répétées ou systématiques.

(46) Nonobstant leurs obligations en matière de protection des données, les fournisseurs de services ne peuvent pas être tenus responsables dans les États membres des préjudices causés à leurs utilisateurs ou à des tiers résultant exclusivement de la conformité de bonne foi à un EPOC ou un EPOC-PR.

(47) En plus des personnes dont les données sont demandées, les fournisseurs de services et les pays tiers peuvent être affectés par la mesure d'enquête. Par courtoisie envers les intérêts souverains des pays tiers, et afin de protéger les personnes concernées et de concilier les obligations contradictoires des fournisseurs de services, le présent instrument prévoit un mécanisme spécifique de contrôle juridictionnel si la conformité avec une injonction européenne de production empêchait les fournisseurs de services de respecter l'obligation légale découlant de la législation d'un État tiers.

(48) À cette fin, chaque fois que le destinataire considère que dans un cas spécifique, l'injonction européenne de production entraînerait la violation d'une obligation légale découlant de la législation d'un pays tiers, il doit en informer l'autorité d'émission par l'intermédiaire d'une objection motivée en utilisant les formulaires fournis. L'autorité d'émission doit alors examiner l'injonction européenne de production à la lumière de l'objection motivée, en tenant compte des mêmes critères que ceux que la juridiction compétente devrait suivre. Lorsque l'autorité décide de maintenir l'injonction, la procédure doit être soumise à la juridiction compétente, comme notifié par l'État membre concerné, qui examine ensuite l'injonction.

(49) Pour déterminer l'existence d'une obligation contradictoire dans les circonstances spécifiques de l'affaire examinée, la juridiction compétente doit s'appuyer sur une expertise externe appropriée si nécessaire, par exemple si le réexamen soulève des questions sur l'interprétation de la législation du pays tiers concerné. Ceci peut inclure la consultation des autorités centrales de ce pays.

(50) Une expertise sur l'interprétation peut également être fournie par des avis d'experts lorsqu'ils sont disponibles. Les informations et la jurisprudence sur l'interprétation des législations de pays tiers et sur les procédures de résolution des conflits de lois dans les États membres doivent être mises à disposition sur une plateforme centrale telle que le projet SIRIUS et/ou le réseau judiciaire européen. Cela devrait permettre aux tribunaux de bénéficier de l'expérience et de l'expertise acquises par d'autres tribunaux sur des questions identiques ou similaires. Cela ne devrait pas empêcher une nouvelle consultation du pays tiers le cas échéant.

(51) Lorsque des obligations contradictoires existent, la juridiction doit déterminer si les dispositions contradictoires du pays tiers interdisent la divulgation des données concernées au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales. Pour procéder à cette évaluation, la juridiction doit évaluer si la

législation du pays tiers, plutôt que d'être destinée à protéger les droits fondamentaux ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, vise manifestement à protéger d'autres intérêts ou vise à protéger des activités illégales contre des demandes des services répressifs dans le contexte d'enquêtes criminelles. Lorsque la juridiction conclut que des dispositions contradictoires du pays tiers interdisent la divulgation des données concernées au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, elle doit consulter le pays tiers via ses autorités centrales, qui sont déjà mises en place aux fins de l'entraide judiciaire dans la plupart des régions du monde. Elle doit fixer un délai pour que le pays tiers présente les objections à l'exécution de l'injonction européenne de production; dans le cas où les autorités du pays tiers ne répondent pas dans le délai (prorogé) malgré un rappel les informant des conséquences de l'absence de réponse, la juridiction confirme l'injonction. Si les autorités du pays tiers s'opposent à la divulgation, la juridiction doit lever l'injonction.

(52) Dans tous les autres cas d'obligations contradictoires, sans rapport avec les droits fondamentaux de la personne ou avec les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, la juridiction doit décider si elle maintient l'injonction européenne de production en prenant en considération un certain nombre d'éléments visant à déterminer la force de la connexion à l'une ou l'autre des deux juridictions concernées, les intérêts respectifs à obtenir ou à empêcher la divulgation des données, et les éventuelles conséquences pour le fournisseur de services qui devra se conformer à l'injonction. Il est important de noter que pour les infractions relevant de la cybercriminalité, le lieu de l'infraction désigne à la fois le ou les lieux où elle a été commise et le ou les lieux où ses effets se sont matérialisés.

(53) Les conditions énoncées à l'article 9 sont également applicables en cas de conflit d'obligations contradictoires découlant de la législation d'un pays tiers. Pendant cette procédure, les données doivent être conservées. Lorsque l'injonction est levée, une nouvelle injonction de conservation peut être émise pour permettre à l'autorité d'émission de demander la production des données par d'autres canaux tels que l'entraide judiciaire.

(54) Il est essentiel que toutes les personnes dont les données sont demandées dans le cadre d'enquêtes ou de procédures pénales aient accès à un recours juridictionnel effectif, conformément à l'article 47 de la charte des droits fondamentaux de l'Union européenne. Pour les personnes suspectées et accusées, le droit à un recours effectif doit être exercé pendant la procédure pénale. Ceci peut affecter la recevabilité ou, le cas échéant, le poids, dans la procédure, de la preuve obtenue de cette manière. Ces personnes bénéficient en outre de toutes les garanties procédurales qui leur sont applicables, tel que le droit à l'information. Les autres personnes, qui ne sont pas suspectées ou accusées, doivent également avoir droit à un recours effectif. Par conséquent, la possibilité de contester la légalité d'une injonction européenne de production, notamment la nécessité et la proportionnalité de la décision, doit au minimum être fournie. Le présent règlement ne peut limiter les motifs possibles de contestation de la légalité de l'injonction. Ces recours doivent être exercés dans l'État d'émission conformément à la législation nationale. Les règles relatives aux mesures provisoires doivent être régies par la législation nationale.

(55) En outre, pendant la procédure d'exécution et le recours ultérieur, le destinataire peut s'opposer à l'exécution d'une injonction européenne de production ou de conservation pour un certain nombre de motifs limités, notamment si l'injonction n'est pas émise ou

validée par une autorité compétente ou s'il apparaît de manière évidente qu'elle viole la charte des droits fondamentaux de l'Union européenne ou est manifestement abusive. Par exemple, une injonction demandant la production de données relatives au contenu appartenant à une catégorie indéterminée de personnes dans une zone géographique ou n'ayant aucun lien avec une procédure pénale concrète ignorerait manifestement les conditions d'émission d'une injonction européenne de production.

(56) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. Conformément à l'article 8, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et à l'article 16, paragraphe 1, du traité FUE, toute personne a droit à la protection des données à caractère personnel la concernant. Lors de la mise en œuvre du présent règlement, les États membres doivent veiller à ce que les données à caractère personnel soient protégées et ne soient traitées qu'en conformité avec le règlement (UE) 2016/679 et la directive (UE) 2016/680.

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

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

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

(60) Afin de répondre efficacement à un éventuel besoin d'amélioration concernant le contenu des EPOC et des EPOC-PR ainsi que du formulaire à utiliser pour fournir des informations sur l'impossibilité d'exécuter l'EPOC ou l'EPOC-PR, le pouvoir d'adopter les actes en conformité avec l'article 290 du traité sur le fonctionnement de l'Union européenne doit être délégué à la Commission afin de modifier les annexes I, II et III du présent règlement. Il est particulièrement important que la Commission procède aux consultations appropriées pendant ses travaux préparatoires, y compris au niveau des experts, et que ces consultations soient réalisées conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[40]. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

(61) Les mesures basées sur le présent règlement ne remplacent pas les décisions d'enquêtes européennes au titre de la directive 2014/41/UE du Parlement européen et du Conseil[41] visant à obtenir des preuves électroniques. Les autorités des États membres doivent choisir l'outil le plus adapté à leur situation; elles peuvent privilégier l'utilisation de la décision d'enquête européenne pour demander plusieurs types différents de mesures d'enquête, y compris, et sans que cela soit limitatif, la production de preuves électroniques d'un autre État membre.

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

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

(64) Conformément à l'article 3 du protocole sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, *[le Royaume-Uni /l'Irlande a notifié son souhait de participer à l'adoption et à l'application du présent règlement] ou [et sans préjudice de l'article 4 dudit protocole, le Royaume-Uni /l'Irlande ne participe pas à l'adoption du présent règlement et n'est pas lié(e) par celui-ci ou soumis(e) à son application.]*

(65) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption du présent règlement et n'est pas lié par celui-ci ou soumis à son application.

---

40 JO L 123 du 12.5.2016, p. 1.

41 Directive 2014/41/EU du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale (JO L 130 du 1.5.2014, p. 1).

(66) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 du Parlement européen et du Conseil[42] et a émis un avis le (...)[43],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre 1: Objet, définitions et champ d'application

Article premier
Objet

1. Le présent règlement définit les règles selon lesquelles une autorité d'un État membre peut ordonner à un fournisseur de services qui propose des services dans l'Union de produire ou de conserver des preuves électroniques, quelle que soit la localisation des données. Le présent règlement est sans préjudice des pouvoirs des autorités nationales de contraindre les fournisseurs de services établis ou représentés sur leur territoire à se conformer à des mesures nationales similaires.

2. Le présent règlement n'a pas pour effet de modifier l'obligation de respecter les droits fondamentaux et les principes juridiques tels qu'ils sont consacrés à l'article 6 du traité sur l'Union européenne, y compris les droits de la défense des personnes faisant l'objet d'une procédure pénale, et toute obligation qui incombe aux autorités répressives ou policières à cet égard demeure inchangée.

Article 2
Définitions

Aux fins du présent règlement, on entend par:

(1) «injonction européenne de production»: une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de produire des preuves électroniques;

(2) «injonction européenne de conservation»: une décision contraignante d'une autorité d'émission d'un État membre imposant à un fournisseur de services proposant des services dans l'Union et établi ou représenté dans un autre État membre de conserver des preuves électroniques en vue d'une demande ultérieure de production;

(3) «fournisseur de services»: toute personne physique ou morale qui fournit une ou plusieurs des catégories de services suivants:

---

42 Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

43 JO C , , p. .

(a) service de communications électroniques tel que défini à l'article 2, paragraphe 4, de la [directive établissant le code des communications électroniques européen];

(b) services de la société de l'information tels que définis à l'article premier, paragraphe1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil[44] pour lesquels le stockage de données est un élément déterminant du service fourni à l'utilisateur, y compris les réseaux sociaux, les marchés en ligne facilitant les transactions entre leurs utilisateurs et autres fournisseurs de services d'hébergement;

(c) nom de domaine internet et services de numérotation IP tels que les fournisseurs d'adresses IP, les registres de noms de domaine, les bureaux d'enregistrement de noms de domaine et les services d'anonymisation et d'enregistrement fiduciaire associés;

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

(a) permettre à des personnes physiques ou morales dans un ou plusieurs État(s) membre(s) d'utiliser les services énumérés au point 3) ci-dessus; et

(b) avoir un lien substantiel avec le ou les États membres visé(s) au point a);

(5) «établissement»: la poursuite effective d'une activité économique pour une durée indéterminée grâce à une infrastructure stable à partir de laquelle l'activité de fourniture de services est réalisée ou une infrastructure stable à partir de laquelle l'entreprise est gérée;

(6) «preuve électronique»: preuve stockée sous forme électronique par un fournisseur de services ou en son nom au moment de la réception d'un certificat d'injonction de production ou de conservation, consistant en données stockées relatives aux abonnés, à l'accès, aux transactions et au contenu;

(7) «données relatives aux abonnés»: toutes les données relatives à:

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

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

(8) «données relatives à l'accès»: les données relatives au début et à la fin d'une session d'accès utilisateur à un service, strictement nécessaires aux seules fins d'identification de l'utilisateur du service, telles que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service, ainsi que l'adresse IP attribuée par le fournisseur de service d'accès à l'internet à l'utilisateur d'un service, les données identifiant l'interface utilisée et l'identifiant de l'utilisateur. Sont incluses les

[44] 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).

métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point g), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques];

(9) «données relatives aux transactions»: les données relatives à la fourniture d'un service proposé par un fournisseur de services, qui servent à fournir des informations contextuelles ou supplémentaires sur ce service, et qui sont générées ou traitées par un système d'information du fournisseur de services, tel que la source et la destination d'un message ou d'un autre type d'interaction, les données sur l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, sauf si ces données constituent des données relatives à l'accès. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point g), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques];

(10) «données relatives au contenu»: toutes les données stockées dans un format numérique tel que du texte, de la voix, des vidéos, des images et du son autres que les données relatives aux abonnés, les données relatives à l'accès ou les données relatives aux transactions;

(11) «système d'information»: un système d'information tel que défini à l'article 2, point a), de la directive 2013/40/UE du Parlement européen et du Conseil[45];

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

(13) «État chargé de la mise en œuvre»: l'État membre dans lequel réside ou est établi le destinataire de l'injonction européenne de production ou de l'injonction européenne de conservation et auquel l'injonction européenne de production et le certificat d'injonction européenne de production ou l'injonction européenne de conservation et le certificat d'injonction européenne de conservation sont transmis pour mise en œuvre;

(14) «autorité chargée de la mise en œuvre»: l'autorité compétente dans l'État chargé de la mise en œuvre à qui l'injonction européenne de production et le certificat d'injonction européenne de production ou l'injonction européenne de conservation et le certificat d'injonction européenne de conservation sont transmis par l'autorité d'émission pour mise en œuvre;

(15) «cas d'urgence»: les situations où il existe une menace imminente pour la vie ou l'intégrité physique d'une personne ou pour une infrastructure critique telle que définie à l'article 2, point a), de la directive 2008/114/CE du Conseil[46].

---

45 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).

46 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).

Article 3
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 pour des procédures pénales, tant durant la phase d'instruction que pendant le procès. Les injonctions peuvent également être émises dans des procédures relatives à une infraction pénale pour laquelle une personne morale peut être tenue responsable ou sanctionnée dans l'État d'émission.

3. Les injonctions prévues par le présent règlement ne peuvent être émises que pour les données relatives à des services tels que définis à l'article 2, paragraphe 3, proposés dans l'Union.

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

Article 4
Autorité d'émission

1. Une injonction européenne de production pour les données relatives aux abonnés et les données relatives à l'accès peut être émise par:

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

   (b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production en vertu du présent règlement, par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

2. Une injonction européenne de production pour des données relatives aux transactions et au contenu peut être émise uniquement par:

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

   (b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de production est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production en vertu du présent règlement, par un juge, une juridiction ou un juge d'instruction dans l'État d'émission.

3. Une injonction européenne de conservation peut être émise par:

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

(b) toute autre autorité compétente telle que définie par l'État d'émission qui, dans le cas d'espèce, agit en sa qualité d'autorité chargée de l'enquête dans les procédures pénales ayant compétence pour ordonner la collecte de preuves conformément à la législation nationale. Cette injonction européenne de conservation est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de conservation en vertu du présent règlement, par un juge, une juridiction, un juge d'instruction ou un procureur dans l'État d'émission.

4. Lorsque l'injonction a été validée par une autorité judiciaire conformément au paragraphe 1, point b), au paragraphe 2, point b), et au paragraphe 3, point b), cette autorité peut également être considérée comme une autorité d'émission aux fins de transmission du certificat d'injonction européenne de production et du certificat d'injonction européenne de conservation.

Article 5

Conditions d'émission d'une injonction européenne de production

1. Une autorité d'émission ne peut émettre une injonction européenne de production que si les conditions énoncées dans le présent article sont remplies.

2. L'injonction européenne de production est nécessaire et proportionnée aux fins de la procédure visée à l'article 3, paragraphe 2, et ne peut être émise que si une mesure similaire est disponible pour la même infraction pénale dans une situation nationale comparable dans l'État d'émission.

3. Les injonctions européennes de production de données relatives aux abonnés ou de données relatives à l'accès peuvent être émises pour toutes les infractions pénales.

4. Les injonctions européennes de production de données relatives aux transactions ou de données relatives au contenu ne peuvent être émises 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 3 ans, ou

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

– les infractions telles que définies aux articles 3, 4 et 5 de la décision-cadre 2001/413/JAI du Conseil[47];

– les infractions telles que définies aux articles 3 à 7 de la directive 2011/93/UE du Parlement européen et du Conseil[48]

– les infractions telles que définies aux articles 3 à 8 de la directive 2013/40/UE du Parlement européen et du Conseil;

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

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

(c) pour les infractions pénales telles que définies aux articles 3 à 12 et 14 de la directive (UE) 2017/541 du Parlement européen et du Conseil[49]

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

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

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

(c) les personnes dont les données sont requises, sauf si l'injonction a pour unique but d'identifier une personne;

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

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

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

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

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

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

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

7. Si l'autorité d'émission a des raisons de croire que les données requises relatives aux transactions ou au contenu sont protégées par des immunités et des privilèges accordés en vertu de la législation de l'État membre du fournisseur de services destinataire ou que leur divulgation peut porter atteinte aux intérêts fondamentaux de cet État membre, tels que la sécurité et la défense nationales, l'autorité d'émission doit demander des éclaircissements avant d'émettre l'injonction européenne de production, notamment en consultant les autorités compétentes de l'État membre concerné, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen. Si l'autorité d'émission constate que les données requises relatives à l'accès, aux transactions ou au contenu sont protégées par ces immunités et privilèges ou que leur divulgation porterait atteinte aux intérêts fondamentaux de l'autre État membre, elle n'émet pas l'injonction européenne de production.

[49] 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).

Article 6

Conditions d'émission d'une injonction européenne de conservation

1. Une autorité d'émission ne peut émettre une injonction européenne de conservation que si les conditions énoncées au présent article sont remplies.

2. Elle peut être émise si elle est nécessaire et proportionnée pour empêcher le retrait, la suppression ou la modification de données en vue d'une demande ultérieure de production de ces données au moyen de l'entraide judiciaire, d'une décision d'enquête européenne ou d'une injonction européenne de production. Les injonctions européennes de conservation de données peuvent être émises pour toutes les infractions pénales.

3. L'injonction européenne de conservation inclut les informations suivantes:

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

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

   (c) les personnes dont les données sont conservées, sauf si l'injonction a pour unique but d'identifier une personne;

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

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

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

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

Article 7

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

1. L'injonction européenne de production et l'injonction européenne de conservation sont adressées directement à un représentant légal désigné par le fournisseur de services aux fins de la collecte de preuves dans le cadre d'une procédure pénale.

2. Si aucun représentant légal spécial n'a été désigné, l'injonction européenne de production et l'injonction européenne de conservation peuvent être adressées à tout établissement du fournisseur de services dans l'Union.

3. Lorsque le représentant légal ne se conforme pas à un certificat d'injonction européenne de production dans un cas d'urgence en vertu de l'article 9, paragraphe 2, ledit certificat peut être adressé à tout établissement du fournisseur de services dans l'Union.

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

Article 8
Certificat d'injonction européenne de production et certificat d'injonction européenne de conservation

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

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

2. L'EPOC ou l'EPOC-PR sont transmis directement par tout moyen susceptible de produire une trace écrite dans des conditions permettant au destinataire d'établir son authenticité.

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

3. L'EPOC contient les informations énumérées à l'article 5, paragraphe 5, points a) à h), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission. Les motifs de la nécessité et de la proportionnalité de la mesure ou d'autres informations concernant les enquêtes ne sont pas inclus.

4. L'EPOC-PR contient les informations énumérées à l'article 6, paragraphe 3, points a) à f), y compris des informations suffisantes pour permettre au destinataire d'identifier et de contacter l'autorité d'émission. Les motifs de la nécessité et de la proportionnalité de la mesure ou d'autres informations concernant les enquêtes ne sont pas inclus.

5. S'il y a lieu, l'EPOC ou l'EPOC-PR est traduit dans une langue officielle de l'Union acceptée par le destinataire. Si aucune langue n'est spécifiée, l'EPOC ou l'EPOC-PR est traduit dans l'une des langues officielles de l'État membre où le représentant légal réside ou est établi.

Article 9
Exécution d'un EPOC

1. Dès réception de l'EPOC, le destinataire veille à ce que les données requises soient transmises directement à l'autorité d'émission ou aux autorités répressives comme indiqué dans l'EPOC au plus tard 10 jours après la réception de l'EPOC, sauf si l'autorité d'émission indique les raisons d'une divulgation anticipée.

2. Dans les cas d'urgence, le destinataire transmet les données requises sans retard injustifié au plus tard 6 heures après la réception de l'EPOC.

3. Si le destinataire ne peut pas respecter son obligation parce que l'EPOC est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour son exécution, le destinataire informe l'autorité d'émission mentionnée dans l'EPOC sans retard injustifié et demande des éclaircissements en utilisant le formulaire figurant à l'annexe III. Il indique à l'autorité d'émission si une

identification et une conservation sont possibles conformément au paragraphe 6. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Les délais prévus aux paragraphes 1 et 2 ne s'appliquent qu'après la fourniture d'éclaircissements.

4. Si le destinataire ne peut pas respecter son obligation pour cause de force majeure ou d'impossibilité de fait qui ne lui est pas imputable ou, le cas échéant, qui n'est pas imputable au fournisseur de services, notamment parce que la personne dont les données sont requises n'est pas leur client, ou que les données ont été supprimées avant la réception de l'EPOC, le destinataire en informe l'autorité d'émission mentionnée dans l'EPOC sans retard injustifié, en expliquant les raisons au moyen du formulaire figurant à l'annexe III. Si les conditions pertinentes sont remplies, l'autorité d'émission retire l'EPOC.

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

   Si le destinataire estime que l'EPOC ne peut pas être exécuté parce qu'il apparaît, sur la base des seules informations contenues dans l'EPOC, que celui-ci enfreint manifestement la Charte des droits fondamentaux de l'Union européenne ou qu'il est manifestement abusif, le destinataire envoie également le formulaire figurant à l'annexe III à l'autorité chargée de la mise en œuvre dans l'État membre du destinataire. Dans ce cas, l'autorité de mise en œuvre compétente peut demander des éclaircissements à l'autorité d'émission de l'injonction européenne de production, soit directement, soit par l'intermédiaire d'Eurojust ou du Réseau judiciaire européen.

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

Article 10
Exécution d'un EPOC-PR

1. Dès réception de l'EPOC-PR, le destinataire conserve les données requises, sans retard injustifié. La conservation prend fin après 60 jours, à moins que l'autorité d'émission ne confirme que la demande de production suivante a été introduite.

2. Si l'autorité d'émission confirme dans le délai fixé au paragraphe 1 que la demande de production suivante a été introduite, le destinataire conserve les données aussi longtemps que nécessaire pour produire les données une fois la demande de production suivante notifiée.

3. Si la conservation n'est plus nécessaire, l'autorité d'émission en informe le destinataire sans retard injustifié.

4. Si le destinataire ne peut pas respecter son obligation parce que le certificat est incomplet, contient des erreurs manifestes ou ne contient pas suffisamment d'informations pour exécuter l'EPOC-PR, le destinataire en informe l'autorité d'émission figurant dans l'EPOC-PR sans retard injustifié et demande des éclaircissements, en utilisant le formulaire figurant à l'annexe III. L'autorité d'émission réagit sans tarder et dans un délai de 5 jours au plus tard. Le destinataire, de son côté, veille à obtenir les éclaircissements nécessaires pour lui permettre de remplir les obligations énoncées au paragraphe 1.

5. Si le destinataire ne peut pas respecter son obligation pour cause de force majeure ou d'impossibilité de fait qui ne lui est pas imputable ou, le cas échéant, qui n'est pas imputable au fournisseur de services, notamment parce que la personne dont les données sont requises n'est pas leur client, ou que les données ont été supprimées avant la réception de l'injonction, il prend contact avec l'autorité d'émission figurant dans l'EPOC-PR sans retard injustifié, en expliquant les raisons, au moyen du formulaire figurant à l'annexe III. Si ces conditions sont remplies, l'autorité d'émission retire l'EPOC-PR.

6. Dans tous les cas où le destinataire ne conserve pas les informations requises, pour d'autres raisons énumérées dans le formulaire de l'annexe III, il en informe l'autorité d'émission sans retard injustifié dans le formulaire figurant à l'annexe III. L'autorité d'émission réexamine l'injonction à la lumière de la justification fournie par le fournisseur de services.

Article 11
Confidentialité et information de l'utilisateur

1. Les destinataires et, le cas échéant, les fournisseurs de services, prennent les mesures nécessaires pour garantir la confidentialité de l'EPOC et de l'EPOC-PR ainsi que des données produites ou conservées et, si l'autorité d'émission le demande, s'abstiennent d'informer la personne dont les données sont requises afin de ne pas entraver la procédure pénale afférente.

2. Si l'autorité d'émission a demandé au destinataire de s'abstenir d'informer la personne dont les données sont requises, elle informe sans retard injustifié la personne dont les données sont requises par l'EPOC au sujet de la production des données. Cette information peut être retardée aussi longtemps que nécessaire et proportionnée pour éviter d'entraver la procédure pénale afférente.

3. Lorsqu'elle informe la personne, l'autorité d'émission fournit des informations sur tous les recours disponibles visés à l'article 17.

Article 12
Remboursement des frais

Le fournisseur de services peut demander à l'État d'émission le remboursement de ses frais, si la législation nationale de l'État d'émission le prévoit pour les injonctions nationales dans des situations similaires, conformément aux dispositions nationales.

Chapitre 3: Sanctions et exécution

Article 13
Sanctions

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

Article 14
Procédure de mise en œuvre

1. Si le destinataire ne respecte pas un EPOC dans les délais ou un EPOC-PR sans fournir de raisons acceptées par l'autorité d'émission, cette dernière peut transférer à l'autorité compétente de l'État chargé de la mise en œuvre l'injonction européenne de production accompagnée de l'EPOC ou l'injonction européenne de conservation accompagnée de l'EPOC-PR ainsi que le formulaire figurant à l'annexe III rempli par le destinataire et tout autre document pertinent en vue de sa mise en œuvre par tout moyen susceptible de garder une trace écrite dans des conditions permettant à l'autorité chargée de la mise en œuvre d'établir son authenticité. À cette fin, l'autorité d'émission traduit la décision, le formulaire et tout autre document les accompagnant dans l'une des langues officielles de cet État membre et informe le destinataire du transfert.

2. Dès réception, l'autorité chargée de la mise en œuvre reconnaît, sans autres formalités, une injonction européenne de production ou une injonction européenne de conservation transmise conformément au paragraphe 1, et prend les mesures nécessaires à sa mise en œuvre, à moins qu'elle ne considère que l'un des motifs prévus aux paragraphes 4 ou 5 s'applique ou que les données concernées sont protégées par une immunité ou un privilège en vertu de sa législation nationale, ou que leur divulgation peut porter atteinte à ses intérêts fondamentaux tels que la sécurité et la défense nationales. L'autorité chargée de la mise en œuvre décide de reconnaître l'injonction sans retard injustifié et au plus tard dans les 5 jours ouvrables suivant la réception de l'injonction.

3. Lorsque l'autorité chargée de la mise en œuvre reconnaît l'injonction, elle enjoint formellement au destinataire de se conformer à l'obligation en question, informe ce dernier de la possibilité de s'opposer à la mise en œuvre en invoquant les motifs énumérés aux paragraphes 4 ou 5, ainsi que des sanctions applicables en cas de non-conformité, et fixe un délai pour qu'il s'y conforme ou qu'il s'y oppose.

4. Le destinataire ne peut s'opposer à la mise en œuvre de l'injonction européenne de production que sur la base des motifs suivants:

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

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

(c) le destinataire n'a pas pu se conformer à l'EPOC en raison d'une impossibilité de fait ou d'un cas de force majeure, 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) sur la base des seules informations contenues dans l'EPOC, il est évident que celui-ci enfreint manifestement la Charte ou qu'il est manifestement abusif.

5. Le destinataire ne peut s'opposer à la mise en œuvre de l'injonction européenne de conservation que sur la base des motifs suivants:

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

(b) le fournisseur de services n'a pas pu se conformer à l'EPOC-PR en raison d'une impossibilité de fait ou d'un cas de force majeure, ou parce que l'EPOC-PR contient des erreurs manifestes;

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

(d) le service n'est pas couvert par le champ d'application du présent règlement;

(e) sur la base des seules informations contenues dans l'EPOC-PR, il est évident que celui-ci enfreint manifestement la Charte ou qu'il est manifestement abusif.

6. En cas d'objection du destinataire, l'autorité chargée de la mise en œuvre décide de mettre en œuvre l'injonction sur la base des informations fournies par le destinataire et, si nécessaire, des informations 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 conformément aux paragraphes 2 et 6, l'autorité chargée de la mise en œuvre consulte l'autorité d'émission par tout moyen approprié. S'il y a lieu, elle demande des informations complémentaires à l'autorité d'émission. L'autorité d'émission répond à toute demande de ce type dans un délai de 5 jours ouvrables.

8. Toutes les décisions sont notifiées immédiatement à l'autorité d'émission et au destinataire par tout moyen permettant de garder une trace écrite.

9. Si l'autorité chargée de la mise en œuvre obtient les données du destinataire, elle les transmet à l'autorité d'émission dans un délai de deux jours ouvrables, sauf si les données concernées sont protégées par une immunité ou un privilège en vertu de sa propre législation nationale ou si elles portent atteinte à ses intérêts fondamentaux tels que la sécurité et la défense nationales. Dans ce cas, elle informe l'autorité d'émission des raisons pour lesquelles les données n'ont pas été transmises.

10. Si le destinataire ne respecte pas ses obligations en vertu d'une injonction reconnue dont la mise en œuvre a été confirmée par l'autorité chargée de la mise en œuvre,

cette autorité inflige une sanction pécuniaire conformément à sa législation nationale. Un recours juridictionnel effectif est disponible contre la décision d'infliger une amende.

Chapitre 4: Recours

Article 15
Procédure de réexamen en cas d'obligations contradictoires basées sur les droits fondamentaux ou les intérêts fondamentaux d'un pays tiers

1. Si le destinataire considère que le respect de l'injonction européenne de production serait contraire aux lois applicables d'un pays tiers interdisant la divulgation des données concernées au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales, il informe l'autorité d'émission des raisons pour lesquelles il ne peut exécuter l'injonction européenne de production conformément à la procédure visée à l'article 9, paragraphe 5.

2. L'objection motivée comprend tous les détails pertinents sur la loi du pays tiers, son applicabilité en l'espèce et la nature de l'obligation contradictoire. Elle ne peut pas être fondée sur le fait que des dispositions similaires concernant les conditions, les formalités et les procédures d'émission d'une injonction de production n'existent pas dans la législation applicable du pays tiers ni sur la seule circonstance que les données sont stockées dans un pays tiers.

3. L'autorité d'émission réexamine l'injonction européenne de production sur la base de l'objection motivée. Si l'autorité d'émission a l'intention de maintenir l'injonction européenne de production, elle demande un réexamen par la juridiction compétente de son État membre. L'exécution de l'injonction est suspendue en attendant la fin de la procédure de réexamen.

   la juridiction compétente évalue d'abord s'il existe un conflit, en examinant

   (a) si la législation du pays tiers s'applique en fonction des circonstances spécifiques de l'affaire en question et, si tel est le cas,

   (b) si la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire en question, interdit la divulgation des données concernées.

4. Pour effectuer cette évaluation, la juridiction devrait déterminer si la législation du pays tiers, plutôt que d'être destinée à protéger les droits fondamentaux ou les intérêts fondamentaux du pays tiers liés à la sécurité ou à la défense nationales, vise manifestement à protéger d'autres intérêts ou vise à protéger des activités illégales des demandes d'application de la loi dans le cadre d'enquêtes pénales.

5. Si la juridiction compétente constate qu'il n'existe pas de conflit pertinent au sens des paragraphes 1 et 4, elle maintient l'injonction. Si la juridiction compétente établit qu'il existe un conflit d'intérêts au sens des paragraphes 1 et 4, elle transmet toutes les informations factuelles et juridiques pertinentes concernant l'affaire, y compris son évaluation, aux autorités centrales du pays tiers concerné, par l'intermédiaire de son autorité centrale nationale, et fixe un délai de 15 jours pour la réponse. Sur demande motivée de l'autorité centrale du pays tiers, le délai peut être prolongé de 30 jours.

6. Si, dans le délai imparti, l'autorité centrale du pays tiers informe la juridiction compétente qu'elle s'oppose à l'exécution de l'injonction européenne de production dans le cas d'espèce, la juridiction compétente lève l'injonction et informe l'autorité d'émission et le destinataire. Si aucune objection n'est reçue dans le délai (prolongé), la juridiction compétente envoie un rappel en donnant à l'autorité centrale du pays tiers 5 jours supplémentaires pour répondre et l'informe des conséquences d'une absence de réponse. Si elle ne reçoit aucune objection dans ce délai supplémentaire, la juridiction compétente maintient l'injonction.

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

Article 16

Procédure de réexamen en cas d'obligations contradictoires basées sur d'autres motifs

1. Si le destinataire considère que le respect de l'injonction européenne de production entrerait en conflit avec la législation applicable d'un pays tiers interdisant la divulgation des données concernées pour d'autres motifs que ceux visés à l'article 15, il informe l'autorité d'émission des raisons pour lesquelles il ne peut exécuter l'injonction européenne de production conformément à la procédure visée à l'article 9, paragraphe 5.

2. L'objection motivée doit inclure toutes les informations pertinentes sur la législation du pays tiers, son applicabilité en l'espèce et la nature de l'obligation contradictoire. Elle ne peut pas être fondée sur le fait que des dispositions similaires concernant les conditions, les formalités et les procédures d'émission d'une injonction de production n'existent pas dans la législation applicable du pays tiers ni sur la seule circonstance que les données sont stockées dans un pays tiers.

3. L'autorité d'émission réexamine l'injonction européenne de production sur la base de l'objection motivée. Si l'autorité d'émission a l'intention de maintenir l'injonction européenne de production, elle demande un réexamen par la juridiction compétente de son État membre. L'exécution de l'injonction est suspendue en attendant la fin de la procédure de réexamen.

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

   (a) si la législation du pays tiers s'applique en fonction des circonstances spécifiques de l'affaire en question et, si tel est le cas,

   (b) si la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire en question, interdit la divulgation des données concernées.

5. Si la juridiction compétente constate qu'il n'existe pas de conflit pertinent au sens des paragraphes 1 et 4, elle maintient l'injonction. Si la juridiction compétente établit que la législation du pays tiers, lorsqu'elle est appliquée aux circonstances particulières de l'affaire examinée, interdit la divulgation des données concernées, elle décide s'il y a lieu de maintenir ou de retirer l'injonction, en particulier sur la base des facteurs suivants:

   (a) l'intérêt protégé par la législation pertinente du pays tiers, y compris l'intérêt du pays tiers d'empêcher la divulgation des données;

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

la localisation, la nationalité et le lieu de résidence de la personne dont les données sont requises et/ou de la(des) victime(s),

le lieu où l'infraction pénale en question a été commise;

(c) le degré de connexion entre le fournisseur de services et le pays tiers en question: dans ce contexte, le lieu de stockage des données en tant que tel ne suffit pas à établir un degré substantiel de connexion;

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

(e) les éventuelles conséquences pour le destinataire ou le fournisseur de services s'il se conforme à l'injonction européenne de production, y compris les sanctions qu'il peut encourir.

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

Article 17
Recours effectifs

1. Les personnes suspectées et accusées dont les données ont été obtenues au moyen d'une injonction européenne de production ont droit à des recours effectifs contre l'injonction européenne de production pendant la procédure pénale pour laquelle l'injonction a été émise, sans préjudice des recours disponibles en vertu de la directive (UE) 2016/680 et du règlement (UE) 2016/679.

2. Lorsque la personne dont les données ont été obtenues n'est pas une personne suspectée ou accusée dans le cadre d'une procédure pénale pour laquelle une injonction a été émise, cette personne a droit à des recours effectifs contre une injonction européenne de production dans l'État d'émission, sans préjudice des recours disponibles en vertu de la directive (UE) 2016/680 et du règlement (UE) 2016/679.

3. Ce droit à un recours effectif est exercé devant une juridiction de l'État d'émission conformément à la législation de cet État et comprend la possibilité de contester la légalité de la mesure, y compris sa nécessité et sa proportionnalité.

4. Sans préjudice de l'article 11, l'autorité d'émission prend les mesures appropriées pour veiller à ce que des informations sur les possibilités de recours prévues par la législation nationale soient fournies et pour garantir qu'elles sont exercées de manière effective.

5. Les mêmes délais ou autres conditions pour la formation d'un recours dans des affaires nationales similaires s'appliquent ici et d'une manière qui garantit l'exercice effectif de ces recours pour les personnes concernées.

6. Sans préjudice des règles de procédure nationales, les États membres garantissent que pour les procédures pénales dans l'État d'émission, les droits de la défense et

l'équité de la procédure sont respectés lors de l'évaluation des preuves obtenues au moyen de l'injonction européenne de production.

Article 18
Garantie des privilèges et des immunités en vertu du droit de l'État chargé de la mise en œuvre

Si les données relatives aux transactions ou les données relatives au contenu obtenues au moyen de l'injonction européenne de production sont protégées par des immunités ou des privilèges en vertu de la législation de l'État membre du destinataire, ou si elles portent atteinte aux intérêts fondamentaux de cet État membre tels que la sécurité et la défense nationales, la juridiction de l'État d'émission garantit que, pendant la procédure pénale pour laquelle l'injonction a été émise, ces motifs sont pris en considération de la même manière que s'ils avaient été prévus par sa législation nationale lors de l'évaluation de la pertinence et de la recevabilité des preuves concernées. La juridiction peut consulter les autorités de l'État membre pertinent, le Réseau judiciaire européen en matière pénale ou Eurojust.

Chapitre 5: Dispositions finales

Article 19
Suivi et rapports

1. Le *[date d'application du présent règlement]* au plus tard, la Commission établit un programme détaillé pour le suivi des résultats, des conséquences et des incidences du présent règlement. Le programme de suivi définit par quels moyens et dans quels intervalles les données et autres éléments de preuve nécessaires seront collectés. Il précise quelles mesures la Commission et les États membres doivent prendre pour collecter et analyser les données et autres preuves.

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

   (a) le nombre d'EPOC et d'EPOC-PR émis par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non);

   (b) le nombre d'EPOC remplis et non remplis par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non);

   (c) pour les EPOC remplis, la durée moyenne pour l'obtention des données requises depuis le moment où l'EPOC est émis jusqu'au moment où il est obtenu, par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non);

   (d) le nombre d'injonctions européenne de production transmises à un État chargé de la mise en œuvre et reçues pour mise en œuvre par type de données requises, les fournisseurs de services destinataires et la situation (cas d'urgence ou non) ainsi que le nombre d'injonctions mises en œuvre;

   (e) le nombre de recours légaux formés contre les injonctions européennes de production dans l'État d'émission et dans l'État chargé de la mise en œuvre par type de données requises.

Article 20
Modifications des certificats et des formulaires

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

Article 21
Exercice de la délégation

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

2. La délégation de pouvoir visée à l'article 20 est conférée pour une durée indéterminée à compter du *[date d'application du présent règlement]*.

3. La délégation de pouvoir visée à l'article 20 peut être révoquée à tout moment par le Parlement européen ou par le Conseil. Une décision de révocation met fin à la délégation de pouvoir spécifiée dans la décision. La révocation prend effet le jour suivant celui de la publication de la décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant d'adopter un acte délégué, la Commission consulte des experts désignés par chaque État membre conformément aux principes énoncés dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016[50].

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

6. Un acte délégué adopté en vertu de l'article 20 n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de 2 mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prorogé de 2 mois à l'initiative du Parlement européen ou du Conseil.

Article 22
Notifications

1. Le *[date d'application du présent règlement]* au plus tard, chaque État membre notifie à la Commission ce qui suit:

   (a) les autorités qui, conformément à sa législation nationale, sont compétentes, conformément à l'article 4, pour émettre et/ou valider des injonctions européennes de production et des injonctions européennes de conservation;

   (b) l'autorité chargée de la mise en œuvre ou les autorités qui sont compétentes pour mettre en œuvre les injonctions européennes de production et les injonctions européennes de conservation pour le compte d'un autre État membre;

[50] JO L 123 du 12.5.2016, p. 13.

(c) les juridictions compétentes pour traiter les objections motivées des destinataires conformément aux articles 15 et 16.

2. La Commission publie les informations reçues au titre du présent article, soit sur un site internet spécifique, soit sur le site internet du Réseau judiciaire européen visé à l'article 9 de la décision 2008/976/JAI du Conseil[51].

Article 23
Rapport avec les décisions d'enquête européennes

Les autorités des États membres peuvent continuer à émettre des décisions d'enquête européennes conformément à la directive 2014/41/UE pour la collecte de preuves qui relèveraient également du champ d'application du présent règlement.

Article 24
Évaluation

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

Article 25
Entrée en vigueur

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

Il s'applique à compter du *[6 mois après son entrée en vigueur]*

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

Fait à Strasbourg, le

Par le Parlement européen	*Par le Conseil*
Le Président	*Le Président*

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