EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
La voix de la profession d'avocat en Europe

Rue Joseph II, 40/8 - B-1000 Bruxelles
T.: +32 (0)2 234 65 10 - ccbe@ccbe.eu - www.ccbe.eu

Position du CCBE sur la proposition de la Commission pour un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

19/10/2018

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays membres, soit plus d'un million d'avocats européens. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.

Le 14 avril 2018, la Commission européenne a publié une proposition de règlement sur les injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

Le CCBE se félicite que la Commission ait tenu compte des différents aspects suggérés par le CCBE lors du processus de consultation précédent. Lors du précédent processus de consultation, le CCBE a déjà publié des commentaires préliminaires qui peuvent être consultés afin d'obtenir davantage d'informations[1]. Le CCBE souhaite détailler davantage ses premières observations sur un certain nombre d'aspects de la proposition.

1. Base juridique, nécessité et proportionnalité

La question principale que pose cette initiative législative est de savoir si l'article 82 (1) du traité sur le fonctionnement de l'Union européenne (TFUE) constitue la base juridique appropriée d'un instrument permettant aux forces de l'ordre d'un État membre d'obliger les entreprises offrant des services de communications électroniques ou de la société de l'information dans l'UE à conserver ou produire des preuves électroniques, quelle que soit leur juridiction et le lieu de conservation des données.

Le principe de reconnaissance mutuelle visé à l'article 82 TFUE est généralement considéré comme étant réservé à la seule coopération entre autorités judiciaires. La proposition envisagée ne concerne toutefois pas les autorités policières ou judiciaires de l'État membre dans lequel se trouve l'entreprise destinataire de la demande. La proposition vise plutôt à conférer une compétence extraterritoriale aux autorités policières ou judiciaires d'un État membre pour qu'elles s'adressent directement à une entité privée dans un autre État membre. En outre, la proposition de règlement prévoit également l'exécution transfrontalière des EPOC[2] et des EPOC-PR[3] qui ont été émis et validés par les seuls procureurs et ne constituent dès lors pas des décisions judiciaires.

Au vu de ces circonstances, le CCBE considère qu'il n'est pas possible que les institutions de l'UE adoptent un instrument juridique permettant aux autorités nationales d'un État membre d'ordonner la production de preuves électroniques à des entités privées dans une autre juridiction. Il est également incertain que la base juridique choisie suffise pour adopter le projet d'article 13 de la proposition, qui oblige l'État membre à prévoir des sanctions pécuniaires en cas de violation des obligations découlant des articles 9, 10 et 11.

Le CCBE considère également que le choix d'un règlement au lieu d'une directive comme instrument juridique pourrait conduire à un changement de paradigme dans le domaine du droit pénal, qui comporte un risque élevé

---

[1] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/FR_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf

[2] **EPOC** signifie « certificat d'**injonction** européenne de production ».

[3] **EPOC-PR** signifie « certificat d'**injonction** européenne de conservation ».

que des normes nationales plus élevées soient abaissées par la législation de l'Union. À cet égard, il convient également de noter que les mesures concernant l'harmonisation des procédures visant à faciliter, entre autres, l'admissibilité mutuelle des preuves entre les États membres ne peuvent, conformément à l'article 82 (2) être adoptées que par voie de directives.

Une autre question importante est de savoir dans quelle mesure la proposition offre une valeur ajoutée par rapport aux traités d'entraide judiciaire et à la décision d'enquête européenne et si elle est accompagnée de garanties suffisantes. En d'autres termes, l'instrument envisagé est-il réellement nécessaire pour atteindre son but et proportionné à l'objectif qu'il est censé atteindre ?

Il ressort de l'exposé des motifs que l'objectif principal de la proposition est d'accélérer la sécurisation et la collecte des preuves électroniques conservées dans une autre juridiction en contournant les autorités judiciaires nationales (disposant souvent de moyens insuffisants) de l'État membre où les éléments de preuve sont conservés. En tant que telle, la proposition instaure essentiellement un mécanisme par lequel les systèmes établis d'entraide judiciaire sont contournés et la protection des droits fondamentaux est déléguée en partie ou en totalité à des parties privées. Le CCBE est en profond désaccord avec cette approche car elle porte atteinte aux devoirs essentiels qu'ont les autorités judiciaires nationales de veiller à ce que les droits de ses citoyens ne soient ni compromis ni affaiblis. Un tel affaiblissement résulte du motif qu'il ne serait plus possible pour les autorités judiciaires nationales de procéder à un contrôle de la légalité des requêtes de coopération judiciaire émanant de l'autorité d'un autre État membre. Le CCBE considère par conséquent qu'au lieu de réduire le rôle et les responsabilités des autorités judiciaires nationales, l'approche plus appropriée consisterait à accélérer les procédures d'entraide judiciaire et de décision d'enquête européenne grâce à la numérisation et en donnant aux autorités nationales les moyens de répondre aux demandes transfrontalières. En l'absence d'une forme quelconque de contrôle de légalité par les autorités judiciaires compétentes de l'État membre dans lequel se trouve son siège, l'entreprise risque d'être tenue de procéder à une divulgation d'une nature ne pouvant normalement pas être exigée dans la juridiction faisant l'objet de la requête. Les petites entités peuvent ne disposer ni des ressources juridiques ni de l'expertise nécessaires pour contester la légalité de l'injonction de production.

Outre la nécessité d'un contrôle de légalité de l'injonction de production de la part des autorités judiciaires compétentes de l'État faisant l'objet de la requête, il peut également s'avérer nécessaire de faire participer à la procédure une personne ou une entité au fait de questions telles que celle de savoir si les éléments de preuve sont susceptibles de relever du secret professionnel de l'avocat. Il s'agirait normalement du responsable du traitement des données (par exemple un cabinet d'avocats). Mais ce n'est pas toujours approprié, en particulier lorsqu'il existe un risque de destruction des éléments de preuve. Toutefois, une fois les données sécurisées, il serait possible et approprié de procéder à un contrôle de légalité avant la production des données ciblées.

Le CCBE propose donc de limiter le champ d'application de la proposition de manière à ne concerner que les injonctions de conservation. Pour ce qui est de la production de preuves électroniques, une injonction de conservation pourrait être suivie du lancement d'une décision d'enquête européenne ou d'une procédure en vertu d'un traité d'entraide judiciaire. Un autre argument en faveur de la limitation de la proposition aux injonctions de conservation se trouve dans les incertitudes procédurales et techniques concernant l'exécution des injonctions de production adressées à des entités privées dans une autre juridiction sans l'intervention des autorités de la juridiction faisant l'objet de la requête, notamment :

- Comment les EPOC doivent-ils être signifiés aux destinataires (par courrier recommandé, électroniquemnet, par un système de distribution particulier, etc.) ?
- Comment les destinataires doivent-ils communiquer les données demandées à l'autorité émettrice (moyens, formats, structure, limites de taille, etc.) ?
- Comment garantir la sécurité de la transaction pour s'assurer que les données sont réelles, exactes et non trafiquées ?
- Comment les destinataires peuvent-ils évaluer l'authenticité et la légalité des EPOC ?

En conséquence des questions évoquées ci-dessus, le CCBE soutient que le champ d'application de la proposition devrait être restreint aux injonctions européennes de conservation et que les objectifs poursuivis par la Commission peuvent être également atteints en recourant, conjointement à la création d'une injonction européenne de conservation, aux procédures prévues dans le cadre de la décision d'enquête européenne et des traités multilatéraux, qui pourraient par conséquent également nécessiter des améliorations.

Néanmoins, au cas où les institutions européennes décideraient d'aller de l'avant avec la proposition dans son état actuel, le CCBE formulerait d'autres observations et propositions de modifications de la proposition qui sont présentées ci-dessous.

2. Contrôle juridictionnel dans l'État membre

Une certaine forme de contrôle juridictionnel dans l'État d'exécution serait nécessaire afin d'assurer une protection suffisante des droits fondamentaux. Le CCBE propose donc que les dispositions de l'article 11(1) de la directive 2014/41 concernant la décision d'enquête européenne soient utilisées pour justifier la non-reconnaissance ou la non-exécution de l'injonction. Si l'information de la personne concernée avant la transmission des données compromet l'enquête, un contrôle juridictionnel significatif de la légalité de la mesure doit au moins être effectué dans l'État membre d'exécution conformément à la législation de cet État. Il serait également possible d'envisager **la création d'un organe judiciaire à l'échelle européenne composé d'autorités de tous les États membres et d'experts indépendants (juges et avocats), qui pourrait être tenu de « donner son feu vert » à toutes les injonctions destinées aux fournisseurs de services et autres entités** (de manière semblable, par exemple, à l'article 15 du projet d'instrument juridique sur la surveillance gouvernementale et la vie privée). L'importance d'un mécanisme de contrôle juridictionnel pour sauvegarder les droits fondamentaux est déjà reconnue dans les instruments européens, par exemple le règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen.

3. Objet

Le premier paragraphe de l'article premier dispose que le règlement concerne la production et la conservation transfrontalières de preuves électroniques sans préciser ce que l'on entend par *preuves*. Afin d'éviter toute divergence d'interprétation quant à l'objet de l'instrument proposé, il est nécessaire que **l'article 2** contienne une définition claire de ce qui est considéré comme *preuves*. La définition pourrait être formulée de la manière suivante :

- « Toutes les données susceptibles d'être utilisées devant les tribunaux dans le cadre d'une affaire pénale spécifique afin d'être utilisées comme éléments de preuve concernant les faits allégués pertinents dans l'affaire. »

4. Champ d'application

Le CCBE considère qu'il est primordial que les injonctions de production et de conservation soient conformes aux exigences de nécessité et de proportionnalité. Par conséquent, **les EPOC et les EPOC-PR ne devraient être délivrés que pour des crimes spécifiques et ne devraient pas l'être dans le but de surveiller des activités criminelles présumées**.

Le considérant 29 indique qu'une injonction européenne de production ne devrait être émise que si elle est 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 ». Cependant, le texte de la proposition de règlement ne contient pas de critères spécifiques pour le contrôle de la nécessité et de la proportionnalité. Par exemple, les conditions d'émission des EPOC/EPOC-PR ne comportent pas de seuil de suspicion suffisant. **Afin d'éviter les abus, les injonctions de production ne doivent être validées par les autorités compétentes que s'il existe des raisons impérieuses donnant lieu à un degré de suspicion suffisant pour justifier la saisie transfrontalière de données**.

L'article 3 (2) indique quant à lui que 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. En outre, il est rappelé à **l'article 5 (2)** que les injonctions européennes de production doivent être nécessaires et proportionnées aux fins de la procédure visée à l'article 3 (2). Le CCBE considère toutefois que le libellé de l'article 3(2) pourrait être interprété d'une manière incompatible avec le libellé du considérant 29, qui fait référence à la nécessité d'émettre des EPOC pour servir « uniquement dans le cas d'espèce ». Compte tenu de l'objet de l'article 2, il est également nécessaire de préciser que le champ

d'application de la proposition devrait être, et est, limité à la production et à la conservation transfrontalières de preuves électroniques, plutôt qu'à la production et à la conservation des données électroniques en général.

Par conséquent, le CCBE propose de modifier le libellé de l'article 3(2) en précisant que les injonctions ne peuvent être émises que dans le but d'obtenir des preuves dans le cadre d'une procédure pénale spécifique. La disposition concernée indiquerait alors ce qui suit : « Les injonctions européennes de production et les injonctions européennes de conservation ne peuvent être émises que ***dans le but d'obtenir des preuves dans le cadre d'une procédure pénale spécifique***, tant durant la phase d'instruction que pendant le procès ».

5. Responsabilité

Selon le considérant 46, les fournisseurs de services ne peuvent être tenus responsables d'aucun préjudice causé par l'exécution injustifiée d'un EPOC ou d'un EPOC-PR tant qu'ils agissent de bonne foi. Le CCBE estime qu'une exclusion de responsabilité aussi vaste pourrait poser problème dans le cas où, par exemple, des renseignements relevant du secret professionnel seraient communiqués à tort aux autorités judiciaires. Une telle exclusion de responsabilité pourrait laisser place à une situation dans laquelle les fournisseurs de services exécutent automatiquement les requêtes sans procéder à l'examen minutieux qui est nécessaire.

Le CCBE estime dès lors que le considérant doit être plus précis, en particulier en ce qui concerne le sens de « bonne foi ».

6. Validation judiciaire

Il semble n'y avoir aucune raison valable pour que les injonctions européennes de production concernant les données relatives aux abonnés et les données d'accès en général ne requièrent pas de validation judiciaire. Il convient de définir plus clairement le type de données considérées comme « données relatives aux abonnés ou données d'accès » afin d'éviter la saisie d'informations qui nécessiteraient normalement un contrôle juridictionnel indépendant conformément aux règles nationales, aux procédures d'entraide judiciaire ou à la décision d'enquête européenne.

Par exemple, les adresses IP ou les interfaces entrent dans plus d'une catégorie, à savoir les données d'accès et les données relatives aux abonnés (**article 2 (7) (b)**). En outre, la définition des données relatives aux abonnés comprend non seulement ce que l'on entend généralement par données relatives aux abonnés (voir l'article 2 (7) (a)), mais également des termes très génériques tels que « type de service [...] y compris les données techniques et les données identifiant les mesures techniques liées ou les interfaces (…) et les données relatives à la validation de l'utilisation du service » (article 2 (7) (b)). Ces termes larges pourraient même inclure des données qui n'ont pas de lien avec le sens habituel du terme « type de service », telles que toutes les caractéristiques techniques du service fourni, rendant ainsi floue la distinction entre les données d'accès et les données relatives aux abonnés. Étant donné que le nouveau règlement proposé relatif à la vie privée et aux communications électroniques[4] utilise un autre type de classification (données et métadonnées de communications électroniques) et que la directive à la vie privée et aux communications électroniques[5] actuellement en vigueur utilise encore une autre définition des données relatives au trafic aux mêmes fins, il est primordial de limiter le nombre de ces termes au minimum nécessaire.

Le fait que la récupération des données relatives aux abonnés et à l'accès en général ne nécessite pas de validation judiciaire va également à l'encontre de l'arrêt rendu récemment par la Cour européenne des droits de l'homme (CEDH) dans l'affaire Benedik contre Slovénie[6] : la Cour a estimé qu'il y avait eu violation de l'article 8 en raison du fait que la police slovène n'avait pas obtenu d'injonction du tribunal pour accéder aux informations relatives aux abonnés associées à une adresse IP dynamique. Selon la Cour, la disposition légale utilisée par la police slovène pour accéder aux informations relatives aux abonnés associées à une adresse IP dynamique sans obtenir d'injonction du tribunal au préalable n'était pas conforme à la norme de la Convention selon laquelle elle doit être « conforme au droit ».

[4] Règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE.
[5] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
[6] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}

Dans l'affaire Tele2/Watson[7], la CJUE a estimé « essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales » (paragraphe 120). La question suivante se pose donc :

- Comment les autorités compétentes peuvent-elles évaluer correctement le bien-fondé d'une demande de délivrance d'injonction européenne de production ?
- Quels renseignements recevront-elles à part le formulaire ?
- Faut-il laisser à chaque État membre le soin de le préciser ou doit-il y avoir des critères et règles en commun ?

Il est important de clarifier que le secret professionnel peut concerner non seulement des données relatives au contenu, mais également d'autres types de données, par exemple les données d'accès. Dans de tels cas, une validation et une supervision judiciaire est nécessaire.

Si le règlement ne donne pas de sécurité absolue quant aux types de données qui entrent dans les diverses catégories, les forces de l'ordre ne sauront pas si elles ont besoin d'une validation judiciaire et les destinataires ne seront pas en mesure d'évaluer si les injonctions européennes de production ont été délivrées en toute légalité.

Il peut également s'avérer nécessaire de faire participer à la procédure une personne au fait de questions telles que celle de savoir si les éléments de preuve sont susceptibles de relever du secret professionnel de l'avocat. Il s'agirait normalement du responsable du traitement des données. Mais ce n'est pas toujours approprié, en particulier lorsqu'il existe un risque de destruction des éléments de preuve.

Le CCBE propose dès lors que les EPOC pour les données relatives aux abonnés et à l'accès soient émises et validées par un juge, un tribunal ou un juge d'instruction et qu'un processus en deux étapes soit requis : premièrement le recours à une injonction de conservation pour obtenir les éléments de preuve avant toute contestation de la demande d'injonction de production, puis l'audience (en cas de contestation) de la demande d'injonction de production.

7. Conditions d'émission d'un certificat d'injonction européenne de production

Exigence de la double incrimination

Dans la deuxième partie des **articles 3(2) et 5(2)**, ce n'est que pour les infractions punissables dans l'État membre d'émission qu'un certificat d'injonction européenne de production peut être délivré. **Le CCBE estime qu'il convient d'exiger que l'infraction en question soit punissable aussi bien dans l'État d'émission que dans l'État membre dans lequel les données sont recherchées**.

Injonctions européennes de production ciblant les données relatives aux abonnés ou à l'accès

Il est également difficilement justifiable que des injonctions européennes de production ciblant les données relatives aux abonnés ou à l'accès puissent également être délivrées pour des infractions mineures sans être limitées aux infractions graves (**article 5(3)**). Cela semble en contradiction avec les arrêts de la CJUE dans l'affaire Tele2/Watson[8] et *Digital Rights Ireland*[9]. **Le CCBE propose donc que les données d'abonnés ou les données d'accès ciblées de l'OEB ne puissent être délivrées que pour des infractions graves**.

Conditions pour les injonctions européennes de production ciblant des données relatives aux transactions ou au contenu

La question se pose de savoir si, dans le cas des injonctions européennes de production ciblant des données relatives aux transactions ou au contenu, une peine privative de liberté d'une durée maximale d'au moins trois

---

[7] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d8409b5427bcc14f3c8fb3fff95b372c57.e34KaxiLc3qMb40Rch0SaxyPaxn0?text=&docid=186492&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=535293

[8] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d8409b5427bcc14f3c8fb3fff95b372c57.e34KaxiLc3qMb40Rch0SaxyPaxn0?text=&docid=186492&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=535293

[9] http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en&type=TXT&ancre=

ans est suffisamment élevée afin d'éviter que l'instrument ne soit utilisé à mauvais escient pour lutter contre de petites infractions. En vertu des codes pénaux des États membres, un très grand nombre d'infractions relèvent de cette catégorie, y compris des infractions qui ne sont pas considérées comme des infractions graves. Les infractions passible d'une peine de moins de trois ans pourraient également être concernées si elles relèvent du champ d'application de l'un des articles mentionnés de la décision-cadre 2001/413/JAI du Conseil, de la directive 2011/93/UE, de la directive 2013/40/UE ou de la directive 2017/541 (article 5 (4)). L'extension du champ d'application à toutes les affaires dont la peine est d'une durée maximale d'au moins trois ans ne rend pas justice à la gravité de l'ingérence. Le CCBE craint que cela s'applique très probablement aux délits mineurs dans de nombreux États membres. **Le CCBE propose dès lors d'inclure une liste d'infractions spécifiques qui ne devrait être limitée qu'aux formes graves de criminalité, tel que le prévoient les arrêts de la CJUE.**

Destinataires des injonctions européennes de production de preuves

En réponse à la consultation publique sur les preuves électroniques, le CCBE a précisé que lorsqu'une injonction de production de preuves est exécutée, une organisation doit être informée, autorisée à évaluer ses droits et ses obligations et, si possible, avoir la possibilité de contester la demande avant la saisie éventuelle de quelconques données.

Cela signifie que les demandes d'accès à la preuve numérique doivent, chaque fois que possible, être adressées aux responsables du traitement des données plutôt qu'aux sous-traitants qui, en particulier lorsque les données relèvent de la responsabilité d'un cabinet d'avocats, offrent de meilleures garanties contre tout partage illégal d'informations relevant du secret professionnel. Les sous-traitants des données ou d'autres intermédiaires n'auraient aucune information sur de nombreux aspects importants du contexte des données recherchées et ne seraient donc pas toujours en mesure d'évaluer la légalité de la demande ni d'autres exigences juridiques devant être respectées.

L'article 5 (6) de la proposition de règlement indique clairement que lorsqu'une injonction européenne concerne les données d'une société ou d'une entité autre qu'une personne physique, les données doivent d'abord être demandées à l'entité en question, à moins que cela ne nuise à l'enquête.

Cette protection est importante car les responsables du traitement des données sont généralement les mieux placés pour examiner et faire valoir tous les droits relatifs aux preuves électroniques qu'il leur est demandé de transmettre.

Les cabinets d'avocats sont concernés par cette disposition et doivent donc être directement pris en compte afin qu'ils soient en mesure d'évaluer les exigences juridiques relatives à ces demandes de données, y compris la possibilité que les données demandées relèvent du secret professionnel. Cette exemption est donc particulièrement importante dans les cas où les données demandées sont conservées par un cabinet d'avocats.

Le CCBE est toutefois inquiet de la formulation très générale qui laisse aux forces de l'ordre une très grande marge de manœuvre pour contourner les responsables du traitement des données. En outre, cet article ne s'applique qu'aux sociétés, alors que dans la plupart des juridictions, les praticiens exerçant seuls (qui constituent la grande majorité des cabinets en Europe) ne sont pas considérés comme des personnes morales. Les avocats exerçant seuls qui sont des personnes physiques ne bénéficieront dès lors pas de la même protection que les cabinets d'avocats. Quelle que soit l'organisation d'un cabinet (avocat exerçant seul ou cabinet d'avocats), le secret professionnel doit toujours être protégé, et toutes les garanties existantes à cet effet doivent être respectées.

Le CCBE propose par conséquent qu'il soit précisé à l'article 5 (6) que l'autorité émettrice est tenue d'exposer et de justifier dûment dans chaque cas pourquoi un EPOC ne peut pas être adressé au responsable du traitement des données (c'est-à-dire la société, les entités autres que les personnes physiques et les membres des professions réglementées) sur le principe d'évaluations significatives et documentées. En outre, l'expression « membres des professions réglementées » devrait figurer dans la même disposition.

Bien que l'article 5 (6) dispose que lorsqu'une injonction européenne de production cible les données d'une société ou d'une entité autre qu'une personne physique, les données doivent être demandées en premier lieu à cette société, ni le libellé de l'article 5 (6) ni celui du considérant 34 ne précisent le type de mesure d'enquête devant être utilisé pour requérir les données détenues par ces entités. Dans l'exposé des motifs, il est indiqué que « Une procédure de décision d'enquête européenne ou d'entraide judiciaire s'avère alors nécessaire si la société n'est pas un fournisseur de services couvert par le champ d'application du présent règlement ». **Afin d'éviter toute insécurité à ce sujet, il est nécessaire de clarifier ce point dans le libellé du règlement proposé.**

Aucune injonction européenne de production de preuves concernant des informations relevant du secret professionnel ne doit être émise ni exécutée

Un autre problème fondamental réside dans le fait que les données connues ou qui auraient dû être connues par l'autorité requérante comme relevant du secret professionnel conformément à la législation de l'État d'émission ou d'exécution sont exclues du champ d'application de l'instrument législatif.

L'article 5 (7) énonce que s'il existe des raisons de croire que les données requises relèvent du secret professionnel, il est nécessaire de demander des éclaircissements auprès des autorités compétentes avant d'émettre l'injonction. Si les données relèvent du secret professionnel, l'injonction européenne de production ne doit pas être délivrée.

La question se pose toutefois de savoir comment les forces de l'ordre peuvent déterminer qui est avocat, en particulier lorsqu'il s'agit d'un avocat d'un autre État membre. Des mesures techniques sont nécessaires pour s'assurer que les forces de l'ordre et les fournisseurs de services sachent que les données sont détenues par des avocats (ainsi que des moyens de vérification de l'identité des avocats). Une solution pragmatique consisterait à exiger que les fournisseurs de services offrent aux avocats la possibilité de préciser qu'ils sont avocats après avoir bien entendu procédé à une vérification minutieuse du statut d'avocat de la personne.

À cet égard, le CCBE peut aider à créer un mécanisme d'identification des avocats à partir de l'outil prototype développé dans le cadre du projet de moteur de recherche d'un avocat 2 (FAL2) pour l'identification des avocats. Cet outil (qui est également utilisé dans le cadre du système e-CODEX) pourrait être adapté à cet usage précis.

En outre, bien que le secret professionnel soit un motif de refus de validation judiciaire (qui doit être pris en compte lors d'un procès pénal : voir l'article 18), il ne constitue pas un motif explicite de refus d'exécuter une injonction européenne de production. **L'article 9 doit donc préciser que le fait que les données requises soient couvertes par le secret professionnel constitue un motif valable de refus d'exécution d'une injonction européenne de production. En outre, sur le formulaire (en annexe), une case supplémentaire doit être ajoutée concernant le secret professionnel et les cas de refus d'exécution d'injonctions européennes de production.**

8. Conditions d'émission d'un certificat d'injonction européenne de conservation

L'article 6 (2) indique ce qui suit au sujet des injonctions de conservation : « 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 ». Toutefois, l'article ne présente aucune garantie contre la conservation généralisée et indifférenciée des données (voir les affaires *Tele2/Watson* et *Digital Rights Ireland*). Il n'existe pas non plus de garanties contre les injonctions de conservation récurrentes qui ne sont pas suivies d'injonctions de production.

Cette disposition doit par conséquent être mise en conformité avec l'arrêt CJUE dans l'affaire Tele2/Watson (voir les paragraphes 108 à 111). Une solution possible consisterait à préciser que l'EPOC-PR doit porter sur la conservation ciblée des données, aux fins de la lutte contre les formes graves de criminalité, à condition que la conservation des données soit limitée au strict nécessaire en ce qui concerne les catégories de données à conserver, les moyens de communication affectés, les personnes concernées ainsi que le délai de conservation adopté.

9. Exécution d'un certificat d'injonction européenne de conservation

Conformément au libellé de l'**article 10**, l'obligation du destinataire de conserver les données demandées cesse d'exister après 60 jours, à moins que l'autorité d'émission confirme avoir « introduit » une injonction européenne de production ultérieure, sans pour autant la « signifier ». Dans une telle situation, aucun délai n'est prévu pour la conservation des données demandées.

Le CCBE considère dès lors nécessaire d'inclure un délai pour les cas où l'autorité d'émission, quelle que soit la raison, s'abstient de signifier l'injonction européenne de production.

10. Motifs de refus d'exécution d'un certificat d'injonction européenne de production

Le CCBE considère que les motifs de refus d'exécuter un EPOC sont trop restrictifs. Outre des raisons techniques ou pratiques (par exemple si l'EPOC est incomplet ou le destinataire ne peut s'y conformer pour un cas de force majeure), le seul motif de non-exécution que le destinataire peut invoquer est le suivant : « 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 ». **Des motifs supplémentaires de refus d'exécution d'une injonction européenne de production doivent donc être prévus, notamment, comme indiqué ci-dessus, l'absence de double incrimination ou le fait que les données demandées relèvent du secret professionnel.**

En matière de procédures litigieuses (au pénal ou au civil), *toute* violation du secret professionnel constitue en soi une violation du droit à un procès équitable au sens de l'article 6 de la CEDH et doit être reconnue comme simple motif suffisant de refus d'exécution d'une injonction européenne de production.

11. Information de la personne concernée

L'obligation d'information prévue à l'**article 11 (2)** peut être très facilement ignorée par les autorités étant donné qu'il est toujours possible de trouver une raison compromettant l'enquête ou la procédure. Il s'agit d'une atteinte grave aux droits des personnes à un procès équitable étant donné que, tant qu'elles ne sont pas au courant de la saisie de leurs données, elles ne peuvent pas faire valoir leurs droits. **Le CCBE estime que l'imposition de restrictions de confidentialité aux injonctions européennes de production doit être soumise à l'approbation d'une autorité judiciaire indépendante et être dans tous les cas dûment motivée et justifiée par l'autorité émettrice à partir d'évaluations significatives et documentées. En ce qui concerne les injonctions européennes de conservation, le CCBE estime également que l'autorité émettrice doit être obligée à informer la personne concernée.**

12. Droits de la défense

Toute proposition relative à la récupération de preuves électronique ne doit pas être considérée uniquement du point de vue de l'accusation. Les droits de la défense doivent également être dûment pris en considération. La proposition ne prend pas correctement en compte l'exigence d'égalité des armes dans les procédures pénales, concept reconnu par la Cour européenne des droits de l'homme dans le cadre du droit à un procès équitable. Alors que les procureurs peuvent émettre des injonctions de production et de conservation, il n'existe aucune disposition permettant à la défense ou à son représentant d'accéder à des éléments de preuve électroniques ou d'en faire la demande.

En outre, la proposition ne prévoit aucune obligation ni ligne directrice pour les destinataires de limiter la transmission de preuves électroniques aux données pertinentes aux fins de la procédure pénale. En conséquence, les forces de l'ordre pourraient être débordées de données. Il n'existe pas non plus de disposition garantissant que la défense ne sera pas accablée par le poids de la preuve électronique, ni que ladite preuve électronique bénéficiera de métadonnées appropriées telles qu'un index et une table des matières. Sans l'aide de ces métadonnées, il est très difficile, voire impossible, que les avocats fassent valoir efficacement les droits de leurs clients.

Le CCBE estime donc que, comme pour la décision d'enquête européenne, les personnes soupçonnées ou poursuivies ou leurs avocats doivent pouvoir demander l'émission d'une injonction européenne de production ou de préservation de manière tout aussi efficace que les procureurs. Sinon, la proposition sape le principe de l'égalité des armes entre l'accusation et la défense, ce qui désavantage considérablement la défense. Par ailleurs, les entités destinataires ne doivent se voir exiger de remettre que les données pertinentes aux fins de l'enquête judiciaire.

13. Recours effectifs et contrôles juridictionnels

En ce qui concerne **l'article 17**, le CCBE considère que les personnes concernées par un **EPOC doivent pouvoir exercer leurs recours non seulement devant le tribunal de l'État d'émission, mais également devant le tribunal**

de l'État membre dans lequel les données sont recherchées. Le CCBE considère qu'il est nécessaire d'étendre également le droit à un recours effectif de l'article 17 aux injonctions européennes de conservation.