EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of the European legal profession

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

Commentaires préliminaires du CCBE sur la proposition d'injonctions européennes de production et de conservation de preuves électroniques en matière pénale

29/06/2018

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. Le CCBE souhaite exprimer ici ses premières observations sur un certain nombre d'aspects de la proposition. Une position plus détaillée suivra en temps voulu.

La question principale que pose cette initiative législative est de savoir si la proposition visant à renforcer les pouvoirs permettant aux autorités chargées d'une enquête d'accéder à des éléments de preuve électroniques au-delà des frontières nationales est assortie de garanties procédurales et de procédures régulières suffisantes. En d'autres termes, certains aspects peuvent-ils compromettre le droit à un procès équitable et, le cas échéant, quelles sont les solutions possibles ?

1. Un mécanisme effectif pour assurer la protection de la confidentialité des communications entre l'avocat et son client. Ce point entraîne les questions suivantes :
    a) À quelles personnes les injonctions doivent-elles être communiquées ?
    b) Dans quelle mesure un contrôle juridictionnel des demandes est-il nécessaire ?
    c) Comment l'efficacité de ce contrôle juridictionnel peut-elle être assurée ?
    d) Les motifs de refus proposés doivent-ils être complétés ?
    e) Les dispositions relatives à l'information doivent-elles être complétées ?
2. La garantie de l'égalité des armes entre l'accusation et la défense.
3. Un contrôle juridictionnel effectif.

Certains commentaires préliminaires sur ces aspects et d'autres encore sont abordés ci-dessous. Ces commentaires devraient constituer la première étape d'un processus dynamique et collaboratif visant à traiter le texte de la proposition au cours du processus législatif. Ils sont à

envisager comme un document préliminaire. Le CCBE présentera des commentaires plus complets et plus détaillés en fonction de la progression du processus législatif.

1. Protection de la confidentialité des communications entre l'avocat et son client

La défense efficace par les avocats des droits de leurs clients dépend de la confiance envers le fait que les communications entre un client et son avocat demeurent confidentielles. Ce principe, généralement appelé secret professionnel ou *legal professional privilege* est reconnu par tous les pays de l'UE et confirmé par la Cour européenne de justice et la Cour européenne des droits de l'homme dans de nombreuses affaires. La violation du secret professionnel constitue, dans certains États membres de l'UE non seulement une violation d'un devoir professionnel, mais également une infraction pénale.

Les documents relevant potentiellement du secret professionnel bénéficieront de la protection renforcée de l'article 8 de la Convention européenne des droits de l'homme (CEDH). En outre, les communications entre un avocat et son client dans le cadre d'une procédure contentieuse (litige pénal ou civil) sont également protégées en vertu de l'article 6 de la CEDH en ce qui concerne le droit à un procès équitable. Les droits énoncés à l'article 6 (contrairement aux droits énoncés à l'article 8) sont absolus dans le sens où aucune limitation ni dérogation n'est possible.

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, les données doivent d'abord être demandées à la société 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. Il conviendrait donc d'ajouter l'expression « membre d'une profession réglementée ». 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.

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

Une autre question clé 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. Certaines mesures techniques semblent 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 vérifications 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 européenne de production.

2. Validation judiciaire

Selon le CCBE, la validation judiciaire par l'État requérant constitue la protection minimale à assurer, d'autant plus que l'autorité du pays destinataire ne vérifiera plus l'injonction (comme c'est le cas pour les procédures d'entraide 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[1] utilise un autre type de classification (données et métadonnées de communications électroniques) et que la directive à la vie privée et aux communications électroniques [2] 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.

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.

3. Degré de suspicion suffisant

Les conditions d'émission d'une injonction européenne de production ou de préservation ne comportent aucun degré de suspicion minimum suffisant (article 5). **Afin d'éviter les abus, les injonctions européennes de production ne doivent être validées par les autorités compétentes que s'il existe des raisons impérieuses donnant lieu à suffisamment de soupçons pour justifier la saisie transfrontalière de données.**

4. Mécanisme effectif pour assurer l'approbation

Pour que les règles d'approbation soient efficaces, il faut qu'il soit possible, le cas échéant, que participe aux procédures une personne au fait de questions telles que la possibilité qu'un élément de preuve soit protégé par le secret professionnel. Cette personne serait normalement le responsable du traitement des données (conformément aux observations ci-dessus). Mais ce n'est pas toujours approprié, en particulier lorsqu'il existe un risque de destruction des éléments de preuve. **Dans de tels cas, il convient d'envisager un processus en deux étapes où une injonction européenne de conservation peut servir à recueillir la preuve avant toute demande d'injonction de production contestée**.

5. Motifs de refus d'exécution

Le CCBE considère que les motifs de refus d'exécuter une injonction européenne de production énoncés à l'**article 9 (5)** sont trop restrictifs. Outre des raisons techniques ou pratiques (par exemple si le certificat d'injonction européenne de production (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

[1] 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.

[2] 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.

de l'Union européenne ou qu'il est *manifestement* abusif ». **Il doit y avoir des motifs plus larges de refus d'exécution d'une injonction européenne de production, notamment l'absence de double incrimination ou, comme indiqué ci-dessus, 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.**

6. Information de la personne concernée

L'article 11 (2) précise que la personne dont les données sont recherchées doit être informée « sans retard injustifié au sujet de la production des données ». Cependant, cette information « peut être retardée aussi longtemps que nécessaire et proportionnée pour éviter d'entraver la procédure pénale afférente ». L'obligation d'information peut donc très facilement être ignorée par les autorités étant donné qu'il est toujours possible de trouver une raison compromettant l'enquête.

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. **L'imposition de restrictions de confidentialité aux injonctions européennes de production doit donc 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.**

7. 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.

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.

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 l'enquête pénale. En conséquence, les forces de l'ordre pourraient être débordées de données. Il n'existe pas non plus de disposition garantissant que les défendeurs ne soient pas accablés par le poids de la preuve électronique, ou 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.

8. Contrôle juridictionnel

Il serait utile d'envisager la mise en place d'un mécanisme efficace de contrôle juridictionnel analogue au mécanisme prévu à l'article 42 du règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée pour la création du Parquet européen, en particulier en ce qui concerne la compétence de la Cour de justice conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne.