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

Recommandations du CCBE sur l'instauration de règles internationales pour l'accès transfrontalier à la preuve électronique

28/02/2019

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million politiques qui concernent les citoyens et les avocats européens.

Ce document constitue la réponse du CCBE à un certain nombre d'évolutions récentes concernant l'instauration de règles internationales pour l'accès transfrontalier à la preuve électronique dans le cadre d'enquêtes pénales, notamment en ce qui concerne la coopération dite directe entre les forces de l'ordre et les prestataires de services.

A. La coopération directe comme variante à la coopération judiciaire

Compte tenu de la fragmentation actuelle de la manière dont l'accès transfrontalier à la preuve électronique est envisagé et traité, le CCBE salue le principe des initiatives visant à créer des cadres juridiques appropriés pour le recueil transfrontalier de ces preuves d'une manière qui offre une sécurité juridique et une plus grande efficacité qu'à l'heure actuelle. Toutefois, ces initiatives devraient s'accompagner de garanties solides pour les personnes dont les données sont consultées, y compris, entre autres garanties, le droit à la protection des données à caractère personnel, à un recours effectif et à un procès équitable, notamment par le respect de la présomption d'innocence et du droit de défense.

Le CCBE ne considère pas que la mise en place de mécanismes de coopération directe entre les forces de l'ordre et les prestataires de services constitue une alternative satisfaisante à la coopération judiciaire entre les forces de l'ordre transfrontalières, ni un moyen nécessaire ou proportionné pour atteindre l'objectif d'efficacité accrue. Ce qu'on appelle la « coopération directe » entre les forces de l'ordre et les prestataires de services n'est pas vraiment un mécanisme de coopération entre parties consentantes étant donné qu'il s'agit d'un moyen par lequel les forces de l'ordre peuvent contraindre les prestataires de services à se conformer à la loi, sans réel contrôle judiciaire. En particulier, elle porte atteinte aux devoirs essentiels des autorités judiciaires nationales de veiller à ce que les droits de leurs citoyens ne soient pas violés, compromis ou sapés. Cette violation résulte du fait que les autorités judiciaires de l'État dans lequel le prestataire de services est situé sont effectivement exclues du processus : elles ne sont pas en mesure d'effectuer un contrôle de légalité des demandes de coopération judiciaire émanant de l'autorité d'un autre État membre. Le CCBE ne peut aucunement soutenir de telles mesures ayant pour effet de réduire le rôle et les responsabilités des autorités judiciaires nationales. Il est plutôt favorable à l'approche consistant à revoir et à améliorer les procédures d'entraide judiciaire actuelles, par exemple en les rendant plus rapides grâce à la numérisation et en prenant des mesures visant à mieux équiper les autorités nationales pour 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 l'entreprise a son siège, il existe un risque que l'entreprise soit tenue de divulguer des données d'une nature qui ne pourrait normalement pas être exigée dans le pays où elles sont demandées. Cela est particulièrement important en ce qui concerne les informations communiquées à titre confidentiel entre les avocats et leurs clients, qui sont juridiquement protégées par le secret professionnel. En outre, les petites entités peuvent ne pas disposer des ressources juridiques et de l'expertise nécessaires pour remettre en question la légalité de l'injonction de production. Par ailleurs, lorsque l'entreprise n'est qu'un simple prestataire de services, elle peut ne pas disposer des connaissances nécessaires ne serait-ce que pour savoir que la demande compromet les droits fondamentaux de la personne concernée.

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. Dans le cas de données à caractère personnel au sens du RGPD, il s'agirait normalement du responsable du traitement des données (par exemple, un cabinet d'avocats) et, dans le cas de données concernant une personne morale (par opposition à une personne physique) (lesquelles données ne relèveraient pas du RGPD), ce serait un « responsable » dans une position analogue. Il est entendu qu'une telle notification peut ne pas toujours être appropriée, en particulier lorsqu'il y a un risque de destruction de preuves quand le responsable du traitement des données apprend qu'une enquête est en cours. Le CCBE reconnaît que de telles situations peuvent survenir de temps à autre et propose que, dans de tels cas, il peut être acceptable de mettre en place un processus de demande de conservation des preuves qui obligerait l'entreprise concernée à prendre des mesures pour conserver ces preuves en attendant la réalisation d'un contrôle de légalité par les autorités judiciaires de l'État où se trouvent les preuves. Une fois les preuves obtenues par le biais d'une injonction de conservation, un contrôle de légalité approprié serait alors effectué avant la production des données ciblées.

Le CCBE propose donc que la coopération directe entre les forces de l'ordre d'une juridiction et les prestataires de services d'autres juridictions soit limitée à la seule obtention d'injonctions de conservation. Pour la production de preuves électroniques, une injonction de conservation pourrait être suivie d'une procédure en vertu d'un traité d'entraide judiciaire. Outre les raisons expliquées ci-dessus, d'autres arguments en faveur de la limitation de la coopération directe aux injonctions de conservation comprennent les incertitudes procédurales et techniques concernant l'exécution de telles injonctions de production adressées à des entités privées dans une autre juridiction sans l'intervention des autorités du lieu où les données sont demandées, notamment :

- Comment les EPOC doivent-ils être signifiés aux destinataires (par courrier recommandé, électroniquement, par un système de distribution particulier, etc.) ?
- Comment les destinataires sont-ils censés soumettre 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 vraies, exactes et non trafiquées ?
- Comment les destinataires peuvent-ils évaluer l'authenticité et la légalité des EPOC ?

En conséquence des questions évoquées ci-dessus et en réponse aux récentes Recommandations de la Commission européenne sur l'ouverture de négociations internationales sur des règles transfrontalières pour l'obtention de preuves électroniques, le CCBE tient à souligner ses préoccupations concernant les évolutions législatives examinés ci-dessous.

B. *CLOUD Act* des États-Unis

Avec l'adoption de la loi états-unienne *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, les organismes d'application de la loi des États-Unis ont maintenant la compétence juridique explicite d'obtenir des données électroniques des entreprises états-uniennes d'informatique en nuage et de communication, quel que soit le lieu où l'entreprise conserve les données. Le *CLOUD Act* propose également un cadre juridique pour accélérer le partage international des données au moyen d'accords exécutifs.

Le CCBE se joint au Parlement européen dans ses préoccupations concernant le *CLOUD Act*, regrettant que les États-Unis aient unilatéralement cherché à étendre la portée territoriale de leurs pouvoirs d'application de la loi, au lieu de recourir à des traités d'entraide judiciaire[1]. Par conséquent, les entreprises offrant des services de communication électronique ou des services de la société de l'information peuvent se trouver confrontées au dilemme d'être obligées de violer soit les obligations juridiques de l'UE (en divulguant des données à caractère personnel conformément à un mandat *CLOUD Act*), soit les obligations juridiques états-uniennes (en ne divulguant pas des données à caractère personnel conformément au droit de l'UE en matière de protection des données, à savoir le Règlement général sur la protection des données).

Bien que le CCBE accueille favorablement les dispositions du *CLOUD Act* qui ont introduit des voies de recours en ce qui concerne les mandats ciblant des ressortissants de pays autres que les États-Unis, il estime que la « motion pour annuler ou modifier » nouvellement introduite est de portée trop étroite. Plus grave encore, la présentation d'une motion d'annulation ou de modification est limitée aux circonstances dans lesquelles seules les lois d'un soi-disant « gouvernement qualifié » pourraient être violées. En outre, la procédure judiciaire n'implique pas l'audition de l'État dans lequel les données saisies sont conservées, ni le fait d'informer la personne concernée après la « saisie » des données. Une autre préoccupation majeure est que le *CLOUD Act* ne prévoit aucun mécanisme approprié pour la protection du secret ou de la confidentialité des éléments de preuve en la possession des avocats, et qui relèvent secret professionnel/*legal professional privilege*. Pour une analyse et une déclaration plus complètes des préoccupations du CCBE à cet égard, voir l'évaluation du CCBE de la loi américaine CLOUD Act.

C. Proposition de la Commission pour un règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

Il est regrettable de constater que l'initiative législative proposée par la Commission européenne en tant que cadre de coopération directe entre les acteurs des forces de l'ordre dans l'UE et les prestataires de services reflète dans une large mesure l'approche adoptée dans le *CLOUD Act* américain et suscite donc des préoccupations similaires.

Bien que cette proposition doive, bien entendu, être interprétée dans un contexte juridique différent, son approche globale est essentiellement la même que celle du *CLOUD Act*. L'objectif principal de la proposition de règlement de la Commission relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale est de permettre aux forces de l'ordre d'un État membre de l'UE d'obliger les entreprises offrant des services de communications électroniques ou de société de l'information dans l'UE à conserver ou produire des preuves électroniques, quelle que soit la juridiction où cette entreprise est établie et où ces données sont stockées.

La position du CCBE concernant cette proposition donne un aperçu détaillé des principaux sujets de préoccupation. La préoccupation fondamentale du CCBE, cependant, est que le règlement proposé

[1] Résolution du Parlement européen du 5 juillet 2018 sur le caractère adéquat de la protection offerte par le bouclier de protection de la vie privée UE/États-Unis (paragraphes 37-38).

introduit un mécanisme par lequel les systèmes établis d'assistance judiciaire sont contournés et la protection des droits fondamentaux est déléguée en partie ou en totalité à des parties privées.

La position du CCBE expose également un certain nombre d'autres questions et préoccupations que le CCBE souhaite voir traitées au cours du processus législatif, notamment en ce qui concerne la protection de la confidentialité des communications avocat-client, la validation judiciaire, les motifs de refus d'exécution de la décision, la nécessité d'un degré suffisant de suspicion pour justifier l'octroi d'une décision, l'importance de l'information des personnes concernées et les droits de la défense.

Le projet de règlement proposé a été publié par la Commission en avril 2018. Le 7 décembre, le Conseil « Justice et affaires intérieures » a approuvé une orientation générale concernant la proposition de règlement. L'approche commune approuvée a été publiée le 12 décembre. Elle contenait un certain nombre de modifications importantes. Par exemple, l'approche commune du Conseil introduit à l'article 7 bis une forme de notification des autorités de l'État membre où les données sont demandées. Cette disposition n'offre toutefois aucune protection significative étant donné que la notification n'a pas d'effet suspensif, l'État membre concerné n'est pas tenu d'intervenir, il n'existe aucun motif pour lequel des objections pourraient être formulées ou la demande pourrait être rejetée, et il n'existe aucune obligation de contrôler la proportionnalité.

L'approche commune du Conseil suggère également de supprimer les motifs pour lesquels les prestataires de services sont autorisés à refuser d'exécuter les injonctions de production. Le CCBE est d'avis qu'au contraire, non seulement ces motifs de refus devraient être préservés, mais devraient également être élargis de manière à inclure également l'absence de double incrimination et le fait que les données demandées relèvent du secret professionnel/*legal professional privilege*.

En outre, l'approche commune du Conseil atténue sensiblement l'obligation d'informer les personnes concernées en précisant qu'elle peut être retardée « pour autant qu'elle constitue une mesure nécessaire et proportionnée ». Cela porte gravement atteinte au droit à un procès équitable des personnes concernées : tant que celles-ci ne savent pas que leurs données ont fait l'objet d'une demande de production, elles ne peuvent faire valoir leurs droits. Comme indiqué dans la position du CCBE, si les injonctions de production de données (par opposition aux injonctions de conservation de données) doivent être autorisées, l'imposition de restrictions de confidentialité sur ces injonctions de production devrait être soumise à l'approbation d'une autorité judiciaire indépendante et dans tous les cas être dûment motivée et justifiée par l'autorité émettrice sur la base d'évaluations significatives et documentées. En outre, ces restrictions de confidentialité ne devraient pas durer plus longtemps qu'il n'est strictement nécessaire. Lorsque les restrictions de confidentialité prennent fin, les personnes concernées devraient être informées et disposer de voies de recours appropriées.

Le CCBE regrette donc qu'au lieu de remédier aux défauts majeurs qui figuraient dans la proposition initiale, l'approche générale du Conseil les exacerbe et sape même les garanties procédurales insuffisantes qui existaient dans la proposition de la Commission.

Dans ce contexte, le CCBE se félicite de ce qui semble être une approche plus sceptique du Parlement européen à l'égard de la proposition. Le CCBE note qu'au lieu de présenter un rapport, la rapporteure pour le dossier, l'eurodéputée Birgit Sippel (S&D, Allemagne), a d'abord publié une série de documents de travail qui évaluent en détail des questions telles que la portée de l'application proposée du projet de règlement et sa relation avec les autres instruments ; l'exécution des injonctions de production et de conservation et le rôle des prestataires de services ; la relation du règlement avec la législation des pays tiers ; les conditions pour émettre des injonctions de production et de conservation ; les garanties et voies de recours (notamment des mesures de protection des données) et la mise en œuvre des injonctions de production et de conservation.

Ces documents de travail serviront de base à la préparation du projet de rapport de la commission LIBE, qui sera produit par le nouveau Parlement après les prochaines élections.

À cet égard, il est important de noter que le deuxième document de travail remet en question la base juridique du règlement proposé sur les éléments de preuve électroniques au motif qu'il va au-delà de l'application actuelle de l'article 82, paragraphe 1, point a), du traité sur le fonctionnement de l'UE en semblant viser à élargir le concept de reconnaissance mutuelle tel qu'il est défini.

Le résultat final du processus législatif reste donc encore très incertain et le CCBE considère qu'il est donc prématuré pour la Commission européenne de chercher à négocier des instruments internationaux en s'appuyant sur la proposition sur la preuve électronique comme point de référence.

D. Deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité

Des évolutions similaires ont également lieu dans le contexte du deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (« Convention de Budapest », STCE n° 185) qui est en cours de négociation. Conformément à son mandat, le deuxième protocole additionnel peut comprendre les éléments suivants :

- Des dispositions pour une entraide judiciaire plus efficace, en particulier :
    - un régime simplifié pour les demandes d'entraide judiciaire concernant les renseignements sur les abonnés ;
    - les injonctions de production internationales ;
    - la coopération directe entre les autorités judiciaires dans le cadre des demandes d'entraide judiciaire ;
    - les enquêtes communes et les équipes communes d'enquête ;
    - les requêtes en langue anglaise ;
    - l'audition audio/vidéo de témoins, de victimes et d'experts ;
    - les procédures d'entraide judiciaire d'urgence ;
- Des dispositions permettant une coopération directe avec les prestataires de services dans d'autres juridictions en ce qui concerne les demandes de renseignements sur les abonnés, les demandes de conservation et les demandes d'urgence ;
- Un cadre plus clair et des garanties plus solides pour les pratiques actuelles d'accès transfrontalier aux données ;
- Des garanties, y compris les exigences en matière de protection des données.

D'après ce qui a été rapporté jusqu'à présent sur l'état actuel des négociations en cours, une approche similaire à celle du *CLOUD Act* des États-Unis et de la proposition de l'UE sur les éléments de preuve électroniques est envisagée. Les préoccupations du CCBE susmentionnées s'appliqueront donc également dans ce contexte.

E. Recommandations du CCBE

La création de mécanismes qui n'ont plus besoin d'un traité d'entraide judiciaire pour permettre aux autorités chargées de l'application de la loi d'obliger les transferts internationaux de données a pour conséquence la suppression des freins et contrepoids qui sont intégrés aux traités d'entraide judiciaire concernant l'échange de données entre l'UE et les États-Unis ou les pays qui sont parties à la Convention de Budapest.

Dans le cadre des négociations du projet d'accord entre l'UE et les États-Unis ainsi que des négociations concernant un deuxième protocole additionnel à la Convention du Conseil de l'Europe

sur la cybercriminalité, le CCBE invite donc instamment les institutions de l'UE à adhérer aux principes suivants afin d'éviter tout conflit potentiel avec le droit européen, de créer des garanties et des voies de recours suffisantes contre les mesures de surveillance de pays tiers et de protéger le secret professionnel/*legal professional privilege* :

1. Reporter la négociation de l'accord proposé entre l'UE et les États-Unis et du deuxième protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité jusqu'à ce que le processus législatif concernant le règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale soit achevé.
2. Garantir le respect des droits fondamentaux, des libertés et des principes généraux du droit de l'UE tels qu'ils sont consacrés par les traités de l'Union européenne, la Charte des droits fondamentaux de l'UE et la Convention européenne des droits de l'homme.
3. Limiter la coopération directe avec les prestataires de services dans d'autres juridictions de manière à ne concerner que les injonctions de conservation, tout en admettant la possibilité qu'une injonction de conservation relative à la preuve électronique puisse être suivie d'une procédure appropriée en vertu d'un traité d'entraide judiciaire pour récupérer cette preuve.

Dans l'hypothèse où les institutions européennes décideraient de procéder à la mise en place d'instruments de coopération directe pour les injonctions internationales de production d'éléments de preuve électroniques, le CCBE les invite instamment à prendre en compte les exigences minimales suivantes auxquelles ces instruments devraient satisfaire, à savoir qu'ils devraient :

1. Établir un mécanisme général de contrôle juridictionnel préalable, y compris un cadre pour la protection du secret professionnel/*legal professional privilege*.
2. Veiller à ce qu'à la suite d'une injonction de production, les données ne soient transférées au pays (tiers) demandeur qu'après notification à une autorité compétente et indépendante d'un État membre de l'UE.
3. Veiller à ce que le prestataire de services destinataire qui traite les données demandées soit informé par l'autorité compétente de l'État membre de l'UE des voies de recours existantes.
4. Prévoir des garanties et des motifs suffisants pour refuser d'exécuter des injonctions internationales de production, en prenant en compte l'absence de double incrimination et le fait que les données demandées relèvent du secret professionnel/*legal professional privilege*. Ces dernières doivent être énoncées explicitement et constituer un motif absolu de refus d'exécution d'une injonction.
5. Veiller à ce que l'imposition de restrictions à la confidentialité des injonctions de production soit soumise à l'approbation d'une autorité judiciaire indépendante et, dans tous les cas, dûment motivée et justifiée par l'autorité émettrice grâce à des évaluations significatives et documentées.
6. Veiller à ce que les restrictions en matière de confidentialité ne durent pas plus longtemps qu'il n'est strictement nécessaire. Lorsque les restrictions de confidentialité prennent fin, les personnes concernées devraient être informées et disposer de voies de recours appropriées.
7. Veiller à ce que les suspects ou les personnes poursuivies ou leur avocat puissent demander l'émission d'injonctions internationales de production ou de conservation d'une manière aussi efficace que possible pour les autorités chargées de l'application de la loi, afin de garantir le respect du principe de l'égalité des armes entre l'accusation et la défense, sans quoi le défendeur est placé dans une position nettement désavantageuse.