

Réponse du CCBE à la consultation publique sur l'amélioration de l'accès transfrontalier aux preuves électroniques en matière pénale

20/10/2017

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, 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.

Dans le présent document, le CCBE répond à la [consultation publique](#) lancée par la Commission sur l'amélioration de l'accès transfrontalier aux preuves électroniques en matière pénale. Cette consultation est importante et le CCBE tient à y répondre. Néanmoins, le questionnaire, qui s'adresse principalement aux autorités publiques et aux fournisseurs de services informatiques, est structuré d'une manière qui n'appelle pas à des réponses liées aux domaines qui sont d'un intérêt particulier pour le CCBE. Par conséquent, le CCBE présente ici sa réponse au questionnaire et formule quelques observations générales supplémentaires sur une éventuelle initiative de l'UE dans le domaine de la preuve électronique.

En avril 2014 a été publiée l'[Étude comparative du CCBE sur la surveillance gouvernementale des données des avocats hébergées dans le nuage](#). Le CCBE y a exprimé ses préoccupations quant à la divergence entre les règles « normales » de perquisition et de saisie d'éléments de preuve et les règles souvent beaucoup plus faibles, voire pratiquement inexistantes, relatives à l'accès aux preuves numériques et à l'interception de transferts de données.

Cette incertitude réglementaire devient particulièrement dangereuse lorsque les données et les communications auxquelles les services répressifs ont accès bénéficient d'une protection particulière dans la loi. Tel est, clairement, le cas des communications entre les avocats et leurs clients. Dans tous les États membres de l'UE, la loi protège de toute divulgation les informations communiquées à titre confidentiel entre un avocat et son client. Ce principe, communément appelé « secret professionnel » ou « *legal professional privilege* », est reconnu depuis des siècles par la plupart des juridictions et affirmé par la Cour de justice européenne dans l'affaire AM&S ([C-155/79](#)).

La protection du secret ou de la confidentialité des données détenues par les avocats qui relèvent de ce secret ou de cette confidentialité est un élément fondateur de l'État de droit. Les régimes de réglementation élaborés de façon indépendante par l'ensemble des juridictions dans l'UE reflètent cette norme fondamentale dans leurs règles respectives applicables dans le déroulement des perquisitions et des saisies d'éléments de preuve dans les cabinets d'avocats. Quelle que soit la diversité parmi ces systèmes (et l'on constate une importante diversité), ils partagent tous cette valeur comme tronc commun.

Les règles n'ont cependant pas toujours suivi les évolutions technologiques. C'est pourquoi, dans certaines juridictions (mais pas dans toutes), les données électroniques conservées dans les locaux d'un fournisseur informatique pour le compte d'un avocat bénéficient d'une protection moindre que les données conservées dans le propre cabinet de l'avocat. Le CCBE ne voit rien qui puisse justifier pareille distinction.

Si la société estime convenablement que ces données doivent bénéficier d'une protection, alors il ne peut y avoir de justification adéquate à une telle discrimination. Dans le milieu informatique actuel, pareille différenciation s'avère également peu naturelle : les utilisateurs ont recours à la même interface

pour accéder aux données, les partager, les communiquer et les stocker ; sans même savoir quand les informations sont envoyées d'un ordinateur à un autre. Il en va de même pour l'avocat qui utilise son ordinateur, que les données électroniques relatives aux clients aient été envoyées en tant que pièces jointes d'un courriel ou simplement partagées avec le destinataire après l'identification de ce dernier.

Un autre domaine d'incertitude réglementaire provient du fait que, dans certains pays, la façon dont la protection des informations des avocats en question est formulée n'établit pas distinctement si les dispositions concernées s'appliquent aux informations stockées chez des fournisseurs de services externes, tels que les fournisseurs de services d'hébergement et d'informatique en nuage. De telles incertitudes pourraient encourager les forces de l'ordre à s'adresser directement au fournisseur de services en nuage afin d'obtenir des informations hébergées sur son ou ses serveurs (sans mandat judiciaire dans certains pays), au lieu de se rendre au cabinet de l'avocat munies d'un mandat délivré par une autorité judiciaire.

Ces problèmes sont d'autant plus intenses en l'absence de moyen technique approprié permettant soit à un fournisseur de services en nuage ou d'hébergement soit à un tiers (tel qu'un organisme ou une puissance étatique) de déterminer si des informations sont protégées par le secret professionnel.

Compte tenu de ces ambiguïtés qui existent au niveau national, il est d'autant plus important que toute initiative de l'UE visant à réglementer l'accès transfrontalier aux preuves numériques garantisse la mise en place de garanties suffisantes pour protéger les droits fondamentaux.

A cet effet, le CCBE appelle les institutions de l'UE à adhérer aux grands principes suivants :

A. Le principe primordial à observer devrait établir que le monde papier et le monde électronique devraient bénéficier d'une protection identique.

Les mêmes principes devraient s'appliquer aux données dans un contexte numérique, comme c'est le cas pour les données qui sont conservées physiquement sur une personne ou dans les locaux d'une organisation. Dans le cas des avocats, cela signifie que, dans la mesure où les règles relatives au monde matériel d'un cabinet d'avocat prévoient notamment la présence de représentants du barreau de l'avocat lors de perquisitions à son cabinet, une disposition similaire devrait alors être prévue pour les perquisitions virtuelles (transnationales). En d'autres termes, le recours à des services de communication électronique ou d'autres services en nuage par les avocats devrait être protégé de la même manière, que le contenu soit stocké dans un centre de données, sur un ordinateur au cabinet de l'avocat ou sur sa propre personne. Cette mesure peut demander davantage de travaux de normalisation en informatique de la part des fournisseurs de services informatiques, y compris des fournisseurs de services d'informatique en nuage, mais le CCBE l'estime nécessaire.

B. Le principe doit établir que la réglementation effective ne puisse pas être raisonnablement contournée. Nous ne devons pas revenir par défaut à une protection minimale.

Il devrait être garanti que lorsqu'un régime strict en vigueur protège les données détenues par les avocats, ce régime ne puisse pas être contourné par les autorités concernées en demandant directement de manière officielle ou officieuse aux fournisseurs de services informatiques des avocats de leur fournir des informations. Lorsqu'un mandat de perquisition est exécuté, l'organisation concernée doit en être informée, elle doit avoir la possibilité d'évaluer ses droits et obligations juridiques et, si possible, de contester la demande avant que des données ne puissent être saisies. Cela implique que les demandes d'accès aux preuves numériques doivent, dans la mesure du possible, toujours être adressées aux responsables des données et non aux responsables du traitement des données.

C. Le principe devrait établir que, quel que soit le régime en vigueur dans un État membre en matière d'accès aux preuves électroniques, il devrait garantir l'inviolabilité des données et des autres éléments de preuves relevant du principe du secret professionnel.

Toutes les protections prévues dans le cadre de la perquisition et de la saisie devraient également s'appliquer si les données sont interceptées et consultées au cours de leur transfert, en tant qu'élément d'une communication, qu'importe si l'entité techniquement chargée de l'interception est un fournisseur de services de communications électroniques, un fournisseur de services informatiques ou une agence étatique agissant directement. Le matériel contenant des informations relevant du secret professionnel

ou du *legal professional privilege* et qui est traité par un service de communications électroniques ou un fournisseur de services en nuage (y compris un fournisseur de services de messagerie électronique) ne devrait pas être accessible aux organismes gouvernementaux.

À cette fin, les forces de l'ordre devraient être tenues d'utiliser tous les moyens technologiques disponibles pour mettre ce qui relève du secret professionnel et du *legal professional privilege* hors de portée des opérations de surveillance. Une solution pragmatique consisterait à exiger que les services de communications électroniques et les fournisseurs de services en nuage offrent aux avocats la possibilité de signaler ces informations, de toute évidence uniquement après avoir soigneusement vérifié si l'utilisateur est effectivement avocat tel qu'il l'affirme. Par exemple, aux Pays-Bas, il existe un système de reconnaissance des numéros de téléphone qui est capable de reconnaître les numéros de téléphone des avocats et de couper la surveillance.

Réponses du CCBE au [questionnaire](#) :

Dans la liste ci-dessous, seules les questions jugées pertinentes pour le CCBE ont été reproduites. La réponse aux questions qui ne figurent pas dans la liste ci-dessous est « sans opinion ».

Partie II : Questions d'ordre général et situation actuelle dans votre pays/entité

26 La Commission européenne devrait-elle proposer des mesures pour améliorer la coopération directe entre les autorités répressives et judiciaires de l'UE et les prestataires de services numériques dont le siège se trouve dans un pays tiers pour autant que des garanties suffisantes soient mises en place pour protéger vos droits fondamentaux ?

- Oui
- Non
- Sans opinion

27 Quels sont les problèmes que peut, selon vous, soulever une initiative de l'UE dans le domaine des preuves électroniques ?

	Très pertinent	Pertinent	Moyennement pertinent	Non pertinent	Sans opinion
* Impact négatif sur les droits (fondamentaux) garantis par le droit national/de l'UE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Perte de souveraineté de votre État membre	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
* Risque de voir un autre pays imposer des obligations similaires aux prestataires de services pour divulguer des preuves électroniques enregistrées dans l'UE (réciprocité)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

28 Quels sont les problèmes que peut, selon vous, soulever une initiative de l'UE dans le domaine des preuves électroniques ?

	Très pertinent	Pertinent	Moyennement pertinent	Non pertinent	Sans opinion
* Moins de compétences par rapport à la situation actuelle	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
* Un paysage d'instruments flou (décision d'enquête européenne, convention de Budapest, entraide judiciaire)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Difficultés pour faire exécuter une demande	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

29 Quels sont les problèmes que peut, selon vous, soulever une initiative de l'UE dans le domaine des preuves électroniques ?

	Très pertinent	Pertinent	Moyennement pertinent	Non pertinent	Sans opinion
* Nature obligatoire	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
* Augmentation du volume des demandes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
* Atteinte à la confiance du client dans vos services	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

33 Quels résultats attendez-vous d'une initiative de l'UE dans le domaine des preuves électroniques ?

	Oui	Non	Sans opinion
* Sécurité juridique	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Des garanties de protection des droits fondamentaux conformément à la charte des droits fondamentaux	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

*** 35 Outre la possibilité de mettre en place un cadre juridique pour les affaires présentant une dimension transfrontière, pensez-vous que l'éventuelle initiative de l'UE devrait aussi couvrir les affaires strictement nationales ?**

- Oui
- Non
- Sans opinion

Partie III. Accès aux preuves électroniques grâce à une demande/injonction de production directement adressée au prestataire de services

58. Une éventuelle initiative de l'UE pourrait permettre aux autorités répressives de demander directement (par une « demande de production ») ou d'enjoindre (par une « injonction de production ») à un prestataire de services situé dans un autre État membre de divulguer des informations particulières sur un utilisateur sans devoir passer par une autorité répressive ou judiciaire dans l'autre État membre. Pensez-vous qu'une initiative de l'UE devrait couvrir

	Oui	Non	Sans opinion
* Une demande directe de production au prestataire de services (mesure volontaire) ?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
* Une injonction directe de production au prestataire de services (mesure contraignante) ?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

59. Si la Commission européenne propose un cadre juridique pour les demandes transfrontières directes aux prestataires de services : dans quelle mesure les conditions suivantes sont-elles pertinentes pour un éventuel instrument transfrontière permettant d'accéder aux preuves électroniques (Veuillez évaluer la pertinence ci-dessous) ?

	Très pertinent	Pertinent	Moyennement pertinent	Non pertinent	Sans opinion
* L'accès direct ne doit être accordé que pour un nombre restreint d'infractions (c'est-à-dire selon le degré de gravité)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* L'acte doit être passible de sanctions dans les deux pays (double incrimination)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Des garanties spécifiques pour les droits fondamentaux	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Notification à l'autre État membre concerné par cette mesure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Possibilité pour l'État membre ayant reçu la notification de contester la mesure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Notification à la personne visée	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Des voies de recours pour la personne concernée	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Partie IV. L'accès direct aux preuves électroniques par le biais d'un système d'information sans qu'un intermédiaire (par ex. un prestataire de services) ne soit impliqué

Un cas de figure qui pourrait se présenter est celui où l'ordinateur portable d'un suspect est fouillé pendant une perquisition effectuée chez lui et un accès à ses dispositifs de stockage virtuels (dans le nuage) est directement possible sur l'ordinateur saisi, mais où on pourrait ne pas savoir où les données sont stockées ou s'il existe une quelconque dimension transfrontière.

64 Selon vous, y a-t-il besoin dans cette situation d'un cadre européen commun ?

- Oui
- Non
- Sans opinion

65 Si la Commission européenne décide de proposer un cadre juridique pour cette situation, que doit prévoir cette proposition ?

	Oui	Non	Sans opinion
* La condition que l'acte soit passible de sanctions dans les deux pays (double incrimination)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Des garanties spécifiques pour les droits fondamentaux	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Notification à l'autre État membre concerné par cette mesure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Possibilité pour l'État membre ayant reçu la notification de contester la mesure	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Notification à la personne visée	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
* Des voies de recours pour la personne concernée (y compris la possibilité de contester la recevabilité des preuves)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>