

La réponse du CCBE à la consultation publique sur l'analyse d'impact relative à la conservation des données par les prestataires de services à des fins de procédures pénales

septembre 2025

Le Conseil des barreaux européens (CCBE) représente les barreaux de 46 pays, soit plus d'un million d'avocats européens. Le CCBE est reconnu comme porte-parole de la profession d'avocat en Europe et représente les intérêts communs des barreaux européens auprès des institutions européennes et internationales. La défense des droits humains et de l'état de droit sont les missions essentielles du CCBE.

Introduction

1. Le CCBE apprécie d'avoir l'occasion de contribuer à cette consultation publique et souhaite mettre à disposition son expertise et sa disponibilité pour participer à l'analyse d'impact prévue sur la mesure proposée en matière de conservation des données.
2. En même temps, le CCBE souhaite exprimer son inquiétude quant au calendrier et à la qualité du questionnaire de consultation publique. En ce qui concerne le calendrier, le CCBE est convaincu qu'une consultation d'une telle importance ne devrait pas être menée pendant la période d'été, où de nombreuses organisations, y compris le CCBE, ont besoin de suffisamment de temps pour consulter leurs membres afin de fournir des commentaires actualisés et représentatifs. En ce qui concerne la qualité, le CCBE a trouvé les questions du questionnaire biaisées et trop générales pour pouvoir donner une image suffisamment nuancée des pratiques actuelles dans le domaine de la conservation des données et de l'application pratique des mesures d'enquête existantes dans l'UE. Cela est d'autant plus important compte tenu des différences entre les législations pénales et les codes de procédure pénale nationaux. Le CCBE constate que les réponses aux questions telles qu'elles sont formulées actuellement donneront une image erronée de la question traitée et des défis qui y sont associés.
3. Par exemple, les questions relatives à l'absence de preuves électroniques ou à l'absence de règles ou d'obligations pertinentes sont trop générales et portent en même temps sur plusieurs aspects. Toute réponse, positive ou négative, nécessiterait plusieurs précisions et nuances supplémentaires. Par exemple, il existe déjà plusieurs mesures d'enquête au niveau de l'UE permettant de demander des preuves électroniques pertinentes, y compris des métadonnées. Toutefois, leur application pratique peut varier d'un contexte à l'autre. Par conséquent, une simple réponse par oui ou par non ne donnerait pas une image suffisamment nuancée et complète, ce qui, à notre avis, est indispensable pour une analyse d'impact.
4. Le CCBE tient à souligner le fait qu'il lui est impossible de répondre à la question relative à la conservation des métadonnées pendant des périodes plus longues et à la conservation de types supplémentaires de métadonnées. La question porte à la fois sur deux aspects et concerne des

sujets différents : l'un concerne la durée de conservation et l'autre les types de données à conserver. Toute réponse donnerait une interprétation erronée des besoins et des défis actuels.

5. Il est également impossible de répondre à la question de savoir si les métadonnées ne devraient être consultées qu'en cas d'infractions graves ou également pour d'autres types d'infractions. En effet, il n'existe pas de définition d'infraction grave au niveau de l'UE étant donné que, comme dans d'autres instruments juridiques relatifs à la conservation des données, la définition de cette notion est laissée à l'appréciation des États membres, dans la mesure où cette définition est conforme au droit de l'Union (par exemple, CJUE 30 avril 2024, n° C-178/22, *Bolzano*, §§ 44-47). En outre, l'accès aux données et leur utilisation ultérieure sont propres à des enquêtes concrètes et à leurs circonstances.
6. La question des risques pour les droits fondamentaux ne semble pas aborder les risques pour le droit à un procès équitable et la violation du principe du secret professionnel.
7. Selon le CCBE, la question du classement des différentes mesures d'enquête en fonction de leur niveau de risque est beaucoup trop générale pour permettre de prendre une telle décision et, aux yeux du CCBE, n'apporte aucune valeur informative supplémentaire au résultat de la consultation. La question des mesures qui seraient moins intrusives tout en permettant une enquête et des poursuites efficaces en matière pénale est également trop générale. Le CCBE est en fait préoccupé par la manière dont les résultats pourraient être interprétés avant les travaux préparatoires à l'instrument législatif proposé. Enfin, le CCBE ne comprend pas pourquoi des solutions telles que « perquisition domiciliaire » ou « saisie d'appareils » ont été ajoutées dans le cadre d'une consultation sur la conservation des métadonnées par les prestataires de services de communication. Nous tenons à souligner que tant la loi que la jurisprudence prévoient que la proportionnalité d'une mesure doit être évaluée en fonction des circonstances. Les questions du questionnaire ne reflètent pas cette exigence légale.
8. Enfin, la question relative à la conservation des données en fonction du type d'enquête semble concerner la situation dans laquelle différents types de données sont conservés à des fins différentes. Dans la pratique, cependant, toutes les données devraient être conservées pendant la même durée jusqu'à ce qu'une demande pertinente soit présentée par l'autorité répressive compétente.
9. C'est pour ces raisons que le CCBE a décidé de ne pas répondre au questionnaire, mais plutôt de présenter nos observations et recommandations dans le présent document.

Remarques générales

1. Le CCBE comprend la nature dynamique des défis auxquels sont confrontées les autorités répressives dans leurs activités de prévention, de détection et d'enquête sur les activités criminelles, compte tenu notamment du rythme des progrès technologiques et du fait qu'une grande partie des activités criminelles laisse une empreinte numérique. Nous soutenons pleinement les objectifs de lutte contre la criminalité et l'adoption de mesures spécifiques pour la prévenir et la combattre.
2. En même temps, le CCBE tient à souligner encore une fois que les nouveaux pouvoirs, parfois élargis, des autorités répressives (s'ils sont jugés souhaitables et proportionnés sur le plan juridique) doivent être accompagnés de garanties adéquates contre les abus, en particulier dans les situations où les cadres juridiques et les traditions des différentes juridictions diffèrent les uns des autres.

3. Le CCBE est particulièrement préoccupé par les menaces potentielles liées à l'accès des autorités répressives aux données, qui peuvent porter atteinte au droit fondamental à la confidentialité des communications entre avocats et clients, ainsi qu'à d'autres droits fondamentaux tels que le droit à la vie privée, le droit à un procès équitable et le droit d'être conseillé, représenté et défendu par un avocat. Cela ajoute une couche de complexité supplémentaire en ce qui concerne la criminalité transfrontalière ou les enquêtes transfrontalières, en particulier en ce qui concerne l'obtention de preuves électroniques.
4. De même, le CCBE est également inquiet de l'incidence potentielle sur le droit à la défense et à un procès équitable, y compris la présomption d'innocence ou le principe de l'égalité des armes. À cette fin, le CCBE a inclus plusieurs commentaires et recommandations qui, il l'espère, aideront la Commission dans son travail d'analyse d'impact et, le cas échéant, sur la mesure législative proposée.

L'importance du secret professionnel

1. La protection du secret professionnel est un droit fondamental et le fondement d'une bonne administration de la justice et du droit à un procès équitable. Elle a été largement reconnue comme telle dans la jurisprudence de la Cour européenne des droits de l'homme (CEDH) et de la Cour de justice de l'Union européenne (CJUE). En particulier, la CEDH déclare dans l'affaire Michaud que : *« [...] si l'article 8 protège la confidentialité de toute « correspondance » entre individus, il accorde une protection renforcée aux échanges entre les avocats et leurs clients. Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : la défense des justiciables. Or un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels. C'est la relation de confiance entre eux, indispensable à l'accomplissement de cette mission, qui est en jeu. En dépend en outre, indirectement mais nécessairement, le respect du droit du justiciable à un procès équitable, notamment en ce qu'il comprend le droit de tout « accusé » de ne pas contribuer à sa propre incrimination. »*¹
2. La CEDH accorde ainsi une protection renforcée au titre de l'article 8 de la Convention européenne des droits humains (CEDH) aux communications relevant de la protection du secret professionnel en tant que droit fondamental. En outre, le CCBE tient à rappeler que, bien que le droit prévu à l'article 8 soit assorti de conditions, le droit à un procès équitable prévu à l'article 6 de la CEDH est absolu et sans conditions. Par conséquent, si une communication protégée par le secret professionnel relève du champ d'application de l'article 6 de la CEDH, alors, compte tenu du caractère absolu de la protection accordée par cet article, il ne devrait y avoir aucune possibilité d'accéder à ces communications.
3. Il existe plusieurs situations dans lesquelles les données conservées par les prestataires de services de communication (et autres) peuvent relever du secret professionnel lorsqu'elles sont saisies par les services répressifs : les données appartiennent à un avocat ou à un cabinet d'avocats ou les données appartiennent à une personne suspecte ou accusée qui communique avec son avocat. L'obligation de conservation indifférenciée des données a de nombreuses répercussions et risques pratiques pour les avocats et leurs clients. Prises dans leur ensemble et analysées, les métadonnées fournissent de nombreuses informations permettant une analyse des schémas qui peut révéler des détails considérables sur la nature des activités de l'avocat et ses relations avec ses clients. Cela comprend :
 - le suivi des communications répétées entre les avocats et leurs clients ;

¹ [Paragraphe 118, Affaire Michaud c. France \(Requête no 12323/11\)](#)

- l'identification des schémas de localisation indiquant quand et où les réunions ont lieu, ainsi que leur durée, la fréquence à laquelle elles ont lieu, etc. ;
 - l'établissement de chronologies des activités des avocats ;
 - la cartographie des réseaux et associations professionnels des avocats ;
 - l'identification de toutes les parties avec lesquelles un avocat communique ;
 - l'identification des sujets ou du contenu potentiels des conseils juridiques (par exemple, à partir des données de l'historique du navigateur ou des métadonnées d'utilisation des applications) ;
 - l'identification des clients (dans certaines juridictions, cela fait partie du secret professionnel) ;
 - la cartographie des relations professionnelles au sein des cabinets d'avocats ; ou
 - le suivi des schémas qui pourraient indiquer des types spécifiques de tâches juridiques ou un travail dans des zones géographiques spécifiques.
4. Une application effrénée et déséquilibrée de ces possibilités technologiques aurait sans aucun doute des répercussions sur le droit à la défense et le droit à un procès équitable.
5. Un exemple concret peut être éclairant à cet égard :

Supposons qu'une personne craigne d'être poursuivie pour avoir commis un acte qui pourrait être punissable en vertu du droit pénal. Elle cherche donc à obtenir des conseils. Elle contacte un avocat par téléphone et lui demande conseil. En raison de la complexité de l'affaire, le client et l'avocat s'échangent plusieurs appels au cours de la journée, et l'avocat finit par informer le client que, selon lui, aucune infraction n'a été commise.

Plus tard, une enquête judiciaire est ouverte et une autorité judiciaire compétente délivre un mandat ordonnant la communication des données d'identité, de trafic et de localisation du suspect.

Les résultats de cette injonction de production montrent que peu après les faits faisant l'objet de l'enquête, le suspect avait contacté un avocat par téléphone à plusieurs reprises. Cette information est ensuite utilisée par la police et les autorités judiciaires pour laisser entendre que le suspect avait apparemment besoin d'une assistance juridique à ce moment-là parce que, hypothétiquement, il savait qu'il avait commis une infraction.

Le résultat est clair : il est évident que le suspect et les autres personnes ayant besoin d'un conseil juridique y réfléchiront à deux fois avant de consulter un avocat et de lui demander conseil.

Il est donc évident qu'il existe un risque d'effet dissuasif lié aux possibilités déséquilibrées et illimitées de conservation et de consultation des données sur les droits de la défense et le droit à un procès équitable en général, et en particulier sur la confidentialité effective des communications entre un avocat et son client.

6. De même, les effets sur le droit à la vie privée sont évidemment en jeu.
7. Ce qui précède est d'autant plus important que, à la suite de plusieurs décisions de la CJUE et de l'exigence selon laquelle la conservation des données doit être ciblée², de nombreux États membres de l'UE autorisent cette conservation, bien qu'à des degrés divers. Si l'on prend l'exemple des limitations géographiques, dans certains pays, les données peuvent être conservées dans des lieux tels que les aéroports ou les grandes gares ferroviaires, qui sont utilisés, entre autres, par les

² Voir par exemple : C-140/20, *Commissaire de l'An Garda Síochána et autres*, [ECLI:EU:C:2022:258](https://eur-lex.europa.eu/eli/cjrep/2022/258)

avocats. En outre, en fonction de leur domaine d'activité, certains avocats peuvent se rendre régulièrement dans des zones considérées comme ayant un taux de criminalité plus élevé. En outre, même si les avocats ne sont pas soumis à de telles mesures de surveillance, leurs clients peuvent l'être, et donc leurs avocats peuvent être identifiés. De plus, la restriction géographique a des implications plus larges et plus générales pour toutes les personnes présentes dans certaines zones, dont les droits peuvent ainsi être violés.

La jurisprudence à l'échelle de l'UE en matière de métadonnées

1. Dans l'affaire *Digital Rights Ireland* (8 avril 2014, C-293/12, C-594/12), la Cour a estimé que la conservation généralisée des données relatives au trafic et à la localisation « est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante » (point 37). Elle a souligné que les métadonnées, prises dans leur ensemble, « sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. » (point 27). La Cour a donc reconnu que la conservation des métadonnées constituait une atteinte particulièrement grave à la vie privée, et non une simple ingérence mineure.
2. Dans l'affaire *Tele2 Sverige* (21 décembre 2016, C-203/15, C-698/15), la Cour a réaffirmé que **les métadonnées permettent de tirer des conclusions très précises** sur la vie privée, « telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » (paragraphe 99-100). Même sans accès au contenu des communications, la conservation des métadonnées « doit être considérée comme particulièrement grave. » (paragraphe 100). Sur cette base, la Cour a estimé que **la conservation générale et sans distinction** des données relatives au trafic et à la localisation était disproportionnée et interdite par l'article 15, paragraphe 1, de la directive « vie privée et communications électroniques » et par la Charte des droits fondamentaux de l'Union européenne.
3. Dans l'affaire *Ministerio Fiscal* (2 octobre 2018, C-207/16), la Cour a déclaré que l'accès aux **données d'identité civile** (par exemple, l'identification de l'abonné derrière une adresse IP dynamique) **ne constitue pas en soi une ingérence « grave »** nécessitant le seuil de la criminalité grave, à condition que cet accès soit nécessaire et proportionné et encadré par des règles claires et précises. Néanmoins, l'accès reste une ingérence qui doit être **fondée sur la loi et bénéficier de garanties appropriées**.
4. Dans l'affaire *Privacy International* (6 octobre 2020, C-623/17), la Cour a estimé que les mesures obligeant les prestataires à transmettre/conservent des données relatives au trafic/à la localisation pour des raisons de sécurité nationale relèvent du champ d'application de la directive « vie privée et communications électroniques » lorsqu'elles contraignent des prestataires privés, et l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de l'article 4, paragraphe 2, du TUE et des articles 7, 8 et 11 et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, s'oppose à toute législation nationale permettant à une autorité publique d'exiger des prestataires de services de communications électroniques qu'ils transmettent de manière générale et sans distinction les données relatives au trafic et à la localisation aux services de sécurité et de renseignement aux fins de la sauvegarde de la sécurité nationale.
5. Dans l'affaire *La Quadrature du Net e.a.* (6 octobre 2020, C-511/18, C-512/18, C-520/18), la Cour a de nouveau souligné le **caractère sensible des métadonnées**, notant que la conservation

générale « peut permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci » (paragraphe 117, citant Digital Rights Ireland et Tele2). La Cour a également établi un lien entre la conservation des métadonnées et **les effets dissuasifs** sur la liberté d'expression (article 11 de la Charte).

6. La Cour a jugé que la conservation des métadonnées n'est autorisée **qu'à titre exceptionnel** (strictement limitée dans le temps et dans sa portée, et sous réserve de garanties solides).
7. Dans *l'affaire Prokuratuur* (2 mars 2021, C-746/18), la Cour a réaffirmé **qu'un contrôle judiciaire ou indépendant** préalable est indispensable avant que les autorités puissent accéder à ces métadonnées.
8. Bien que l'affaire portait sur **l'accès** aux métadonnées, la Cour a souligné que l'accès aux **données de trafic/de localisation conservées** a un **effet sérieux** et que « l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, **sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès aux dites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.** » (paragraphe 45).
9. Dans *l'affaire G.D. c. Commissioner of An Garda Síochána* (5 avril 2022, C-140/20), la Cour a réaffirmé que **les métadonnées relatives au trafic et à la localisation** sont très révélatrices et que leur conservation sans discernement est disproportionnée. En revanche, **les données d'identité civile** sont traitées différemment : la conservation du nom et de l'adresse de l'abonné est autorisée car elles ne permettent pas, en elles-mêmes, de tirer des conclusions précises sur la vie privée. La Cour a ainsi opéré une **distinction** selon laquelle l'accès aux données relatives au trafic ou à la localisation entraîne une ingérence grave dans les droits fondamentaux, tandis que l'accès aux données d'identité/IP est moins intrusif, ce qui permettrait dans ce dernier cas la conservation avec des garanties appropriées.
10. Dans *l'affaire Bundesrepublik Deutschland c. SpaceNet & Telekom Deutschland* (20 septembre 2022, C-793/19, C-794/19), la Cour a confirmé que la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation est interdite, sous réserve du cas exceptionnel de mesures législatives justifiées par une menace grave pour la sécurité nationale, tout en distinguant cela de la conservation généralisée autorisée d'autres types de données, telles que les adresses IP et les données d'identité civile, dans des conditions strictes. Il n'y a donc pas d'interdiction pour les mesures législatives qui, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves pour la sécurité publique, prévoient :
 - la conservation ciblée des données relatives au trafic et à la localisation, limitée, sur la base de facteurs objectifs et non discriminatoires, en fonction des catégories de personnes concernées ou d'un critère géographique, pour une durée limitée à ce qui est strictement nécessaire, mais pouvant être prolongée ;

- la conservation généralisée et sans distinction des adresses IP attribuées à la source d'une connexion Internet pendant une durée limitée au strict nécessaire ;
 - la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de systèmes de communications électroniques ; et
 - le recours à une instruction imposant aux prestataires de services de communications électroniques, par une décision de l'autorité compétente sous réserve de contrôle judiciaire effectif, de procéder, pendant une période déterminée, à la conservation accélérée des données relatives au trafic et à la localisation détenues par ces prestataires de services,
 - à condition que ces mesures garantissent, au moyen de règles claires et précises, que la conservation des données en question soit sous réserve du respect des conditions de fond et de procédure applicables et que les personnes concernées bénéficient de garanties effectives contre les risques d'abus.
11. Dans l'affaire *A.G.* (7 septembre 2023, C-162/22), la Cour a précisé que les données conservées en vertu de la directive « vie privée et communications électroniques » à des fins pénales ne peuvent être réutilisées pour d'autres procédures (par exemple, des fautes administratives). La Cour précise que « de telles données ne sauraient, après avoir été conservées et mises à la disposition des autorités compétentes aux fins de la lutte contre la criminalité grave, être transmises à d'autres autorités et utilisées afin de réaliser des objectifs, tels que, comme en l'occurrence, la lutte contre des fautes de service apparentées à la corruption, qui sont d'une importance moindre, dans la hiérarchie des objectifs d'intérêt général, que celui de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique » (paragraphe 41).
12. Dans l'affaire *La Quadrature du Net (II) – HADOPI* (30 avril 2024, C-470/21), la Cour a affiné la distinction entre les différents types de métadonnées : **les adresses IP** peuvent être conservées de manière générale pour lutter contre les délits en général, *mais uniquement* si des garanties permettent d'assurer qu'elles **ne peuvent pas être associées**, au stade de la conservation, à **des métadonnées (données relatives au trafic/à la localisation)**. Le raisonnement repose sur l'idée que **les métadonnées sont particulièrement sensibles**, car une fois combinées avec des données d'identité/IP, elles permettent de dresser le profil de la vie privée.
13. La Cour a ainsi élevé la « **non-corrélabilité** » au stade de la conservation au rang de principe clé : les métadonnées doivent rester logiquement/techniquement séparées des autres identifiants, sauf si des garanties strictes et la proportionnalité sont respectées, en déclarant qu'« un État membre qui entend imposer aux prestataires de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général doit s'assurer que les modalités de conservation de ces données soient de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées, dans le respect de la directive 2002/58, qui permettrait de tirer des conclusions précises sur la vie privée des personnes dont les données seraient ainsi conservées » (paragraphe 83).
14. Dans l'affaire *Procura della Repubblica di Bolzano* (30 avril 2024, C-178/22), la Cour a précisé que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte, ne s'oppose pas à une législation nationale autorisant l'accès, sur décision judiciaire, aux données de trafic ou de localisation conservées pour enquêter sur des délits passibles d'une peine maximale d'au moins trois ans d'emprisonnement, à condition que cet accès soit fondé sur des pièces suffisantes, qu'il soit pertinent pour établir les faits et qu'il soit soumis à un contrôle préalable effectif par une juridiction ayant le pouvoir discrétionnaire de le refuser si le

délict n'est manifestement pas grave. La Cour a ainsi réaffirmé que cet accès constitue une ingérence grave dans les droits fondamentaux et n'est admissible que s'il respecte les principes de proportionnalité, de nécessité et de contrôle judiciaire strict.

Considérations relatives à la base juridique de l'instrument proposé

1. Conformément au principe d'attribution, l'UE ne peut légiférer que si les traités lui ont conféré une compétence. La question centrale est de savoir s'il existe une base juridique pour les actes de l'Union en matière de conservation des données et, dans l'affirmative, quelles sont les dispositions applicables.
2. Au départ, la directive 2006/24/CE sur la conservation des données s'appuyait sur l'article 114, paragraphe 1, du TFUE (compétence en matière de marché intérieur). La Cour de justice de l'Union européenne a confirmé cette base juridique, estimant que la directive réglementait les obligations des entreprises de télécommunications plutôt que les activités répressives. Cependant, la Cour a ensuite annulé la directive dans son arrêt *Digital Rights Ireland* (affaires jointes C-293/12 et C-594/12) en raison d'une ingérence disproportionnée dans le droit à la vie privée. Pour respecter le principe de proportionnalité, la nouvelle législation devrait limiter l'accès des autorités répressives aux affaires de criminalité grave. Dans un premier temps, de telles règles ne relèveraient pas de l'article 114 du TFUE étant donné qu'elles concernent la sécurité publique et le droit pénal et relèvent donc de la compétence des États membres. Cela crée un dilemme juridique : la proportionnalité exige des règles en matière d'accès, mais celles-ci semblent dépasser le champ d'application de l'article 114.
3. Toutefois, un examen plus approfondi révèle que ce dilemme n'est peut-être pas aussi strict qu'on le suggère parfois. Si l'article 114 ne peut servir de base pour réglementer les activités des autorités répressives nationales (ce qui nécessiterait en effet l'article 87 TFUE), les obligations des prestataires de services de communications électroniques peuvent être définies en vertu de l'article 114. En d'autres termes, le législateur européen n'est peut-être pas en mesure de prescrire aux États membres *qui* peut accéder aux données et *dans quelles conditions matérielles*, mais il peut limiter les obligations de divulgation imposées aux prestataires de services, circonscrivant ainsi indirectement le champ d'accès.
4. Cette interprétation peut être étayée par la jurisprudence de la CJUE relative à l'article 15, paragraphe 1, de la directive 2002/58 sur la vie privée et les communications électroniques, qui repose elle-même sur la compétence en matière de marché intérieur. Dans l'affaire *Tele2 Sverige AB* (C-203/15, points 72 et suivants), la Cour a précisé que le droit de l'Union européenne peut fixer des limites aux obligations de conservation et de divulgation des prestataires sans pour autant réglementer directement les activités des autorités publiques. De même, l'ancienne directive sur la conservation des données comprenait déjà un article 4 qui ne précisait pas quelles autorités auraient accès aux données ni les conditions détaillées de cet accès, mais qui clarifiait que l'accès devait toujours être limité et conforme aux normes de nécessité, de proportionnalité et de droits fondamentaux de l'UE. Ces clarifications peuvent être justifiées en tant que mesures relatives au marché intérieur, garantissant des obligations uniformes pour les prestataires tout en respectant les droits fondamentaux.
5. Une autre base juridique réside dans l'article 87, paragraphe 2, point a), du TFUE, sous le titre « Espace de liberté, de sécurité et de justice ». Cette disposition autorise des mesures relatives à la collecte, à la conservation et à l'échange d'informations à des fins de coopération policière. Toutefois, elle ne couvre que la coopération transfrontalière, et non l'application purement nationale de la loi, ce qui reflète la délégation limitée de souveraineté des États membres en matière pénale.

6. En conclusion, un acte de l'Union fondé uniquement sur l'article 114 du TFUE peut réglementer les obligations de conservation des données pour les entreprises et peut également, conformément au principe de proportionnalité, inclure des précisions indiquant que les données conservées ne peuvent pas être soumises à un accès illimité. Les dispositions allant plus loin, en particulier celles qui concernent directement les pouvoirs des autorités répressives, nécessitent l'article 87, paragraphe 2, point a), du TFUE et sont limitées à la coopération transfrontalière. Ainsi, la compétence de l'UE dans ce domaine reste fragmentée et limitée sur le plan juridique, mais le champ d'application de l'article 114 TFUE ne doit pas être interprété de manière trop restrictive : il peut soutenir des règles qui restreignent indirectement l'accès en définissant les obligations et les limitations qui incombent aux prestataires de services.

Recommandations

1. Le CCBE a déjà élaboré en détail les principes qui doivent être reflétés dans toute législation réglementant l'accès aux données des citoyens, y compris des avocats³. Il souhaite en rappeler certains ici et ajouter plusieurs considérations qui, à son avis, doivent être examinées plus en détail dans l'analyse d'impact qui accompagnera l'instrument législatif proposé.
2. Tout d'abord, le CCBE recommande que **des dispositions explicites protègent le secret professionnel** et que l'instrument législatif proposé introduise une **norme minimale pour cette protection**. Compte tenu de la nature extrêmement sensible de ces droits fondamentaux, qui sont indissociables des garanties nationales de l'état de droit, une approche d'harmonisation maximale devrait être exclue dans ce domaine. Deuxièmement, nous recommandons que l'instrument proposé comprenne diverses dispositions qui donnent effet à cette protection et garantissent **le respect des droits fondamentaux, en particulier le droit à un procès équitable et le droit à la défense**.
3. À cette fin, il convient de **définir de manière claire et précise**, entre autres, les types de données à conserver par les prestataires et les situations dans lesquelles l'accès aux données est exercé par les autorités répressives. En particulier, les concepts de sécurité nationale, d'infraction ou crime grave, d'extrémisme, de terrorisme ou de crise en tant qu'éléments justificatifs de l'accès et du traitement des communications devraient être définis avec suffisamment de précision et de clarté.
4. Tout accès aux données à caractère personnel par les autorités répressives doit être soumis à une **autorisation préalable** délivrée par un tribunal. Le juge qui approuve une demande de collecte ne devrait pas être le même que, le cas échéant, le juge qui supervise la mise en œuvre de tout accès pour lequel une autorisation a pu être accordée. En aucun cas, le juge qui a donné son accord ne peut être le juge dans une procédure pénale ultérieure fondée sur les données acquises. Dans les juridictions qui prévoient un rôle pour le bâtonnier ou une autre autorité du barreau, par exemple en étant présent lors des perquisitions ou en étant informé de l'accès prévu aux données, les règles spéciales régissant l'octroi ou l'exécution du mandat doivent continuer à être respectées. De telles dispositions existent en Belgique, en France, en Italie et en Slovénie.
5. Par conséquent, il devrait y avoir **des dispositions spécifiques régissant l'identification et le traitement obligatoires des informations qui sont ou peuvent être protégées par le secret professionnel** pendant l'enquête, afin d'éliminer le risque qu'elles puissent être utilisées par la suite. Cette utilisation concerne à la fois l'introduction comme pièce dans une procédure, mais aussi l'utilisation indirecte pour obtenir des preuves légales étant donné qu'une violation illégale

³ Voir les [Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance](#) et les [Recommandations du CCBE sur la protection des droits fondamentaux dans le contexte de la « sécurité nationale »](#).

des droits fondamentaux ne devrait pas être récompensée. Les autorités répressives devraient également être tenues d'utiliser tous les moyens qu'il est possible d'invoquer pour exclure ces informations du champ d'application des demandes d'accès. De telles procédures devraient également exister du côté des prestataires de services (*infra*, n° 11).

6. Dans les cas où les avocats eux-mêmes sont soupçonnés d'avoir commis une infraction et où un mandat est délivré pour accéder aux communications entre l'avocat et son client, il est nécessaire d'assurer une supervision à toutes les étapes de l'enquête, au cas par cas, et d'avoir une possibilité d'impliquer son association professionnelle. Cela permet de garantir la protection du secret professionnel de tous les clients des avocats dont les affaires ne sont pas liées à l'enquête en question.
7. En ce qui concerne les protections spécifiques du secret professionnel prévues par la législation, la Cour européenne des droits de l'homme, dans l'affaire *Denysyuk et autres c. Ukraine* (requêtes n° 22790/19 et trois autres), a critiqué le fait que les procédures régissant les mesures d'enquête secrètes ne contenaient aucune ligne directrice spécifique détaillant le contenu des dispositions légales relatives à la protection des communications entre avocats et clients. Elle a également commenté qu'il n'apparaissait pas clairement qu'il existait d'autres instruments accessibles au public dans le droit interne qui définissaient les garanties spécifiques à appliquer et les procédures à suivre dans les cas où les autorités interceptaient accidentellement une conversation privilégiée entre un suspect et son avocat dans le cadre d'écoutes téléphoniques, de surveillances audio ou d'autres opérations similaires. La Cour a fait remarquer qu'il n'était donc pas clair de savoir comment les communications privilégiées devaient être identifiées, traitées et détruites afin de satisfaire aux exigences du droit interne. La Cour a également commenté que les autorités judiciaires, qui ont autorisé les mesures d'enquête secrètes, n'avaient pas compétence pour superviser la mise en œuvre de leurs décisions, que leurs pouvoirs se limitaient à la phase d'autorisation initiale et qu'il n'existait aucune autre autorité suffisamment indépendante de celles impliquées dans l'affaire pour poursuivre le délit présumé⁴. La Cour a conclu à une violation de l'article 8.
8. Dans ce contexte, **le CCBE recommande d'examiner plus en détail les effets de la mesure proposée sur les procédures et le traitement des communications relevant du secret professionnel compte tenu des différences de protection au niveau national.**
9. La législation ne devrait pas empêcher les avocats de protéger de manière adéquate la confidentialité de leurs communications avec leurs clients (par exemple en utilisant des services qui ne nécessitent pas la conservation de métadonnées) et ne devrait pas donner aux agences publiques ou aux autorités répressives un accès privilégié à ces données, qu'elles soient chiffrées ou non.
10. La législation doit également prévoir la possibilité pour les prestataires de refuser de transmettre les données demandées aux autorités répressives au motif qu'elles relèvent du secret professionnel.
11. Toute information consultée en application des instruments juridiques de l'UE, mais sans autorisation judiciaire (préalable) et en violation du principe du secret professionnel de l'avocat devrait, en application d'une disposition juridique spécifique à cet égard, être jugée irrecevable devant un tribunal afin de garantir l'efficacité des garanties qui devraient être incluses. La CJUE a constaté dans l'affaire *Encrochat* que : « en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie

⁴ [DENYSYUK ET AUTRES c. UKRAINE](#), (requêtes n° 22790/19 et trois autres, voir la liste en annexe), 13 février 2025 (paragraphe 111 et 112)

procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (voir, en ce sens, arrêts du 16 décembre 1976, *Rewe-Zentralfinanz* et *Rewe-Zentral*, 33/76, EU:C:1976:188, point 5, ainsi que du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 223) » (M.N., 30 avril 2024, C-670/22, point 129).

12. Toutefois, le simple fait de prévoir des règles d'exclusion des preuves en cas d'utilisation non autorisée par les autorités répressives des métadonnées relatives aux communications entre avocats et clients n'est pas une panacée.
13. Même lorsque les métadonnées ne sont pas officiellement utilisées comme preuves à l'encontre d'un suspect, elles peuvent néanmoins être utilisées par les autorités répressives et judiciaires pour affiner leur obtention de preuves.
14. Dans certains systèmes juridiques, cela est même explicitement autorisé, en utilisant ces données comme des « renseignements », sans en divulguer l'origine. Par exemple, la loi belge autorise une telle utilisation des renseignements qui « permet d'orienter l'enquête dans une certaine direction et, par la suite, d'obtenir des preuves de manière indépendante » :
 - à prendre en considération, sans préciser comment les renseignements ont été obtenus, pour autant qu'il soit démontré que cela n'a pas été fait de manière illégale (Cass. 10 septembre 2013, AR P.13.0376.N, Arr. Cass. 2013, n° 434) ; et
 - en principe, même être utilisés s'il est établi ou rendu plausible que les renseignements ont été obtenus illégalement, à moins qu'il ne soit démontré *in concreto* que leur utilisation constitue une violation de l'article 6 CEDH (Cass. 27 juin 2017, AR P.15.0814.N, Arr. Cass. 2017, n° 423).
15. Cette jurisprudence nationale et la possibilité d'utiliser de manière informelle des métadonnées collectées illégalement concernant les communications entre les avocats et leurs clients pour orienter une enquête pénale constituent clairement une menace pour la protection pratique et effective des garanties précitées.
16. Cela montre clairement qu'il est non seulement nécessaire d'empêcher que ces métadonnées protégées soient *utilisées comme pièces* par les autorités répressives et judiciaires, mais aussi qu'elles leur soient *communiquées*. Cette responsabilité devrait incomber à la fois aux autorités répressives et aux prestataires de services qui conservent les métadonnées en question.
17. Tout matériel obtenu légalement ne devrait être utilisé qu'aux fins pour lesquelles l'autorisation de l'organe de contrôle a été accordée, les exceptions devant être clairement identifiées par la loi conformément aux droits fondamentaux.
18. Afin d'assurer une protection juridique efficace contre la surveillance illégale, il est nécessaire que des recours juridiques soient mis à la disposition des avocats et de leurs clients qui ont fait l'objet d'une surveillance illégale. En outre, le cas échéant, des sanctions devraient être imposées aux personnes et aux agences ayant procédé à cette surveillance illégale.
19. En particulier, une fois que la mise en place de mesures de surveillance a été révélée, les avocats et leurs clients doivent avoir le droit d'être informés des données collectées à la suite d'une surveillance directe ou indirecte. De telles dispositions existent déjà à l'article 13 de la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif ou à l'article 13

du règlement sur les preuves électroniques (ce dernier s'appuyant sur les dispositions pertinentes de ladite directive). Le CCBE note que la première évaluation de la directive a observé que : « *Les personnes physiques utilisent également de plus en plus leur droit d'introduire des réclamations auprès des autorités de contrôle de la protection des données, notamment dans les cas où les autorités compétentes limitent l'exercice des droits des personnes concernées. Plus d'un tiers des autorités de contrôle de la protection des données ont signalé une augmentation du nombre de réclamations reçues à la suite de la transposition de la directive en matière de protection des données dans le domaine répressif dans leur État membre. Certaines des réclamations les plus fréquentes reçues par les autorités de contrôle de la protection des données concernaient la limitation du droit d'accès, le droit de rectification ou d'effacement, et le droit à l'information et les limitations y afférentes. Elles ont été suivies de réclamations relatives au principe de limitation de la conservation, qui exige des autorités compétentes qu'elles ne conservent pas les données à caractère personnel plus longtemps que nécessaire, et au droit à l'information.* »⁵ En outre, la Cour de justice de l'Union européenne (CJUE), dans l'affaire *CG c. Bezirkshauptmannschaft Landeck*, a souligné l'importance du droit à l'information en tant que pilier fondamental du droit à un recours effectif. Nous recommandons que l'analyse d'impact inclue des considérations plus approfondies sur la manière dont le droit à l'information peut être exercé dans le contexte de l'instrument législatif proposé. Cela est d'autant plus important dans le cas des instruments transfrontaliers de récupération des preuves, qui ajoutent une couche de complexité supplémentaire aux efforts de la défense pour examiner les preuves étrangères.

20. En outre, ces dispositions sont importantes étant donné que toute la défense repose sur les preuves et la capacité d'évaluer leur légalité et leur recevabilité. C'est pourquoi un accès précoce au dossier et, dans ce cas, aux informations sur les données consultées et à quel effet, est essentiel pour examiner les preuves et assurer une défense efficace. C'est pourquoi les principes de notification et d'information des personnes concernées sont essentiels : ils permettent de disposer du temps nécessaire pour préparer la défense.
21. Une fois qu'il a été révélé que les données d'une personne ont été consultées, les avocats et les clients concernés devraient pouvoir contester la légalité de ces mesures devant un tribunal. À l'instar de ce que le CCBE a préconisé dans le cadre du règlement sur les preuves électroniques⁶, les personnes concernées par une injonction d'accès aux données devraient pouvoir exercer leurs recours devant le tribunal de leur pays de résidence. Le CCBE recommande donc que l'analyse d'impact examine plus en détail comment garantir l'efficacité des recours dans l'instrument proposé.
22. Toutes les autorités répressives qui ont été reconnues coupables d'avoir accédé illégalement à des données devraient être tenues responsables et se voir infliger des sanctions.
23. Le CCBE recommande que l'analyse d'impact examine plus en détail la question de la présomption d'innocence et les effets de l'instrument proposé sur ce droit important. Dans certains cas, l'accès aux données sur la base de la localisation géographique ou des antécédents criminels peut avoir des effets sur l'ensemble des personnes concernées. De plus, dans un monde numérisé, la plupart des contacts, quels qu'ils soient, laissent des traces sous forme de (méta)données. L'analyse d'impact devrait évaluer comment éviter durablement les soupçons injustifiés et la pénalisation de citoyens innocents.

⁵ [Premier rapport sur l'application et le fonctionnement de la directive \(UE\) 2016/680 en matière de protection des données dans le domaine répressif](#), Bruxelles, 25.7.2022, COM(2022) 364 final, page 22

⁶ Voir la [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](#) (2018)

24. Le CCBE recommande également que l'instrument proposé comporte des dispositions établissant des conditions claires et prévisibles pour la délivrance d'injonctions/mandats de production, telles qu'une justification appropriée, un soupçon raisonnable et un contrôle juridictionnel. À cette fin, les concepts de sécurité nationale, d'extrémisme, de terrorisme ou de crise en tant qu'éléments justificatifs du traitement des données à caractère personnel devraient être définis avec suffisamment de précision et de clarté. Les demandes de données devraient être précises en termes de destinataires/sujets/types de données demandées/indication claire de la période pour laquelle les données sont demandées.