EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
La voix des avocats européens

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

Position du CCBE sur la proposition de règlement sur le développement de l'informatique en nuage et de l'IA (CADA)

19 novembre 2026

Le CCBE accueille favorablement la proposition de règlement de la Commission européenne sur le développement de l'informatique en nuage et de l'IA (CADA)[1], notamment en ce qu'elle vise à renforcer l'écosystème européen de l'informatique en nuage et de l'IA, à réduire les dépendances stratégiques en matière d'infrastructures numériques critiques et à instaurer un cadre d'évaluation unique à l'échelle de l'Union européenne pour la souveraineté en matière d'informatique en nuage et d'IA.

1. Remarques générales

Le CCBE soutient globalement l'orientation de la proposition, dès lors qu'elle reconnaît que certaines fonctions publiques, telles que le système judiciaire, nécessitent un niveau plus élevé de maîtrise opérationnelle, de résilience, de sécurité et de protection contre les dépendances extérieures. Le CCBE réaffirme sa position antérieure selon laquelle le système judiciaire doit être considéré comme une infrastructure critique pour nos sociétés, essentielle à la cohésion sociale, à l'État de droit et à la résilience démocratique. Il doit dès lors bénéficier du soutien, de la protection et des ressources nécessaires.[2] Par ailleurs, la proposition ne doit pas porter atteinte au principe d'indépendance du système judiciaire.

1.1. Indépendance du système judiciaire

Le CCBE souligne que, pour préserver son indépendance, le système judiciaire doit conserver une maîtrise effective des services numériques critiques et fonctionner dans un environnement offrant de solides garanties, notamment en ce qui concerne la protection des données sensibles et/ou couvertes par le secret professionnel et la continuité du service.

---

[1] Proposition de règlement sur le développement de l'informatique en nuage et de l'IA (CADA) : https://digital-strategy.ec.europa.eu/fr/library/proposal-cloud-and-ai-development-act-cada (3 juin 2026)

[2] Réponse du CCBE à l'appel à contributions concernant la législation européenne sur le développement de l'informatique en nuage et de l'IA : https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20250701_CCBE-response-to-the-call-for-evidence-for-the-EU-Cloud-and-AI-Development-Act.pdf (juillet 2025)

Cette maîtrise suppose, à tout le moins, de savoir clairement qui exploite le service, où les données sont traitées et stockées, qui peut accéder aux systèmes, quelles lois régissent les obligations du prestataire en matière de communication de données aux autorités répressives et quelles lois encadrent sa capacité à assurer la continuité du service.

À mesure que l'administration de la justice devient davantage tributaire des infrastructures numériques, les questions relatives à la continuité, à la gouvernance, à la propriété, au droit applicable, à la sous-traitance et à l'architecture technique de ces services prennent de l'importance au regard de l'État de droit. En effet, une rupture de la continuité du service, l'impossibilité d'accéder aux dossiers, la divulgation illicite ou insuffisamment encadrée d'informations confidentielles, ou encore la dépendance à l'égard d'un prestataire soumis à des obligations juridiques contradictoires peuvent compromettre non seulement l'efficacité administrative, mais aussi l'accès à la justice, l'égalité des armes, les droits de la défense et la confidentialité des communications entre l'avocat et son client.

1.2. Infrastructure souveraine et écosystème réglementaire

Le CCBE souligne que les infrastructures souveraines doivent s'accompagner du respect des principes de légalité, de nécessité et de proportionnalité, d'un contrôle indépendant, de voies de recours effectives et de garanties spécifiques pour les informations couvertes par le secret professionnel ou par le privilège juridique professionnel. Le CCBE estime que les exigences prévues par la CADA devraient être conçues de manière à soutenir et à renforcer les alternatives européennes existantes. Elles ne devraient pas imposer d'obligations qui ne peuvent pas encore être pleinement respectées dans la pratique, car cela risquerait de pénaliser de manière disproportionnée les avocats et les autres acteurs de la justice, qui dépendent des prestataires de services disponibles et ne sont pas en mesure de développer eux-mêmes les alternatives technologiques nécessaires.

Si la souveraineté technologique européenne peut réduire certaines dépendances à l'égard de pays tiers ainsi que certains risques de conflits de lois, elle ne garantit pas, à elle seule, le respect de l'État de droit. Elle doit donc s'inscrire dans un cadre plus large respectueux des droits fondamentaux.

Du point de vue de la profession d'avocat, les questions suivantes revêtent une importance particulière :

- la mise au point de moyens techniques permettant d'identifier, dans un environnement en ligne, les données couvertes par le secret professionnel ou *legal professional privilege*;
- la protection de ces données contre toute divulgation et leur exclusion du champ des injonctions de production ou de conservation, conformément aux droits fondamentaux applicables et à la jurisprudence de la CJUE et de la Cour EDH ; et
- l'identification et l'authentification des avocats en tant que professionnels habilités au sein des systèmes de justice en ligne.

Toutefois, afin que les clients puissent communiquer avec leur avocat sans craindre que les autorités répressives ou d'autres tiers apprennent qu'ils ont pris contact avec lui, il est essentiel que l'identification des avocats et des informations couvertes par le secret professionnel ou *legal professional privilege* demeure facultative, tout en permettant d'exclure ces informations des demandes d'accès. Cette identification ne doit constituer une obligation ni en droit ni dans les faits.

L'expérience des membres du CCBE concernant les systèmes nationaux de justice en ligne montre également qu'une infrastructure nationale exploitée par l'État ne garantit pas, à elle seule, la fiabilité du système ni le respect des droits procéduraux. Dans ce contexte, **le CCBE souligne que la souveraineté fonctionnelle doit englober la fiabilité des systèmes et le respect des exigences procédurales applicables, la transparence quant à leur disponibilité, la responsabilité en cas de défaillance ainsi que des conséquences procédurales clairement définies pour les utilisateurs lorsqu'un système est défaillant.**

1.3. Protection du secret professionnel et du privilège juridique professionnel dans l'environnement numérique

En tant que collaborateurs indépendants de l'administration de la justice, les avocats figurent parmi les principaux utilisateurs des infrastructures numériques du système judiciaire et constituent, à ce titre, des parties prenantes essentielles.[3] Le CCBE estime donc indispensable que le futur écosystème européen de l'informatique en nuage et de l'intelligence artificielle soit développé de manière à reconnaître le statut particulier des données couvertes par le secret professionnel et le privilège juridique professionnel. La confidentialité des communications entre l'avocat et son client ne constitue pas une simple obligation professionnelle imposée aux avocats. Reconnue de longue date dans toute l'Europe, elle est essentielle à une représentation juridique effective. Elle permet aux clients de communiquer librement et en toute franchise avec leur avocat, afin que celui-ci puisse leur fournir des conseils juridiques précis et assurer efficacement leur représentation. Elle constitue ainsi une garantie essentielle du droit à un procès équitable. Le secret professionnel et *legal professional privilege* sont solidement ancrés dans la jurisprudence et les instruments juridiques européens et reconnus dans l'ensemble des États membres de l'Union européenne. Ils constituent des principes fondamentaux de la profession d'avocat, consacrés par la Charte des principes essentiels de l'avocat européen et le Code de déontologie des avocats européens du CCBE.

Dans ce contexte, il importe de souligner que la protection conférée par le secret professionnel ou *legal professional privilege* va bien au-delà des garanties prévues pour les données à caractère personnel par le règlement (UE) 2016/679 (RGPD). Alors que le RGPD protège les données à caractère personnel relatives à des personnes physiques identifiables, le secret professionnel ou *legal professional privilege* protège le contenu même des communications entre l'avocat et son client, qu'elles comportent ou non des données à caractère personnel. Par conséquent, le seul respect des règles relatives à la protection des données ne garantit pas la confidentialité exigée par le secret professionnel : les éléments couverts par le secret professionnel ou *legal professional privilege* peuvent notamment comprendre des informations relatives à des entreprises, des secrets d'affaires ou des communications concernant des personnes morales, dont aucun ne relève du champ d'application du RGPD, mais qui demeurent tous pleinement protégés. **Toute infrastructure européenne d'informatique en nuage et d'intelligence artificielle utilisée dans l'écosystème judiciaire doit donc être conçue de manière à empêcher les fournisseurs de services d'informatique en nuage ou d'IA d'accéder aux données couvertes par le privilège juridique professionnel, de les**

[3] Voir, par exemple : affaire C-432/23, Barreau de Luxembourg (ECLI:EU:C:2024:791)

analyser, de les exploiter ou de les utiliser à des fins d'entraînement, et de manière à ce que cette protection soit également opposable aux autorités de pays tiers. Traiter les données couvertes par le secret professionnel ou *legal professional privilege* comme une simple catégorie particulière de données à caractère personnel ne satisferait pas aux exigences établies par la jurisprudence de la Cour de justice et risquerait de porter atteinte à la substance même du droit à un procès équitable.

1.4. Accès aux données couvertes par le secret professionnel ou le privilège juridique professionnel

Le CCBE recommande que la reconnaissance des pays tiers tienne compte de la question de savoir si leur législation protège les communications entre l'avocat et son client contre tout accès imposé par les autorités répressives. L'article 18 porte sur les pays tiers associés et prévoit que la Commission peut, par voie d'actes d'exécution, désigner les pays tiers dont les fournisseurs de services d'informatique en nuage peuvent faire l'objet d'un audit au regard des critères d'assurance de l'Union de niveau 3. Cette disposition permet, lorsque la Commission le juge approprié, d'évaluer certains fournisseurs sous contrôle non européen au titre du cadre de l'Union relatif à la souveraineté en matière d'informatique en nuage. À cette fin, l'article prévoit six conditions cumulatives auxquelles le pays tiers doit satisfaire, énumérées aux points a) à f). Le CCBE est favorable à l'inclusion, parmi ces critères, de l'absence de mesures susceptibles de contraindre un fournisseur à interrompre ou à perturber un service, ou à divulguer des données, sans les garanties prévues par le droit de l'Union. Une décision d'adéquation adoptée au titre du règlement général sur la protection des données (RGPD) ne couvre pas, à elle seule, la question du secret professionnel.

1.5. Mécanisme d'identification des données des avocats

Le CCBE préconise la mise au point de moyens techniques permettant d'identifier les données détenues par les avocats. La difficulté pratique consiste à permettre aux autorités répressives de déterminer que des données sont détenues par un avocat, en particulier lorsque celui-ci est établi dans un autre État membre. Sans mécanisme fiable d'identification des avocats et de vérification de leur qualité professionnelle, les garanties applicables risquent d'être difficiles à mettre en œuvre efficacement dans la pratique. Des mesures techniques appropriées devraient donc permettre tant aux autorités répressives qu'aux prestataires de services de reconnaître qu'un compte appartient à un avocat. Une solution envisageable consisterait à imposer aux prestataires de services de permettre aux avocats d'indiquer leur qualité professionnelle, sous réserve d'une vérification fiable de celle-ci. Il est toutefois essentiel que l'identification des avocats et des informations couvertes par le secret professionnel ou *legal professional privilege* demeure facultative, tout en permettant d'exclure ces informations des demandes d'accès, et qu'elle ne soit imposée ni comme une obligation légale ni comme une obligation de fait (comme expliqué à la section 1.2).

1.6. Application extraterritoriale des législations de pays tiers

Le CCBE souligne également que, lorsqu'un prestataire est soumis à la législation d'un pays tiers, les données détenues dans le secteur judiciaire ainsi que les informations détenues par les avocats et leurs clients peuvent être exposées à des risques difficilement conciliables avec les exigences du droit de l'Union. Ces risques concernent non seulement l'accès non autorisé aux données, mais aussi

des risques opérationnels, tels que les interruptions de service, l'exposition à des sanctions, la dépendance à l'égard d'un fournisseur, l'impossibilité de migrer vers d'autres prestataires ou encore la dépendance à l'égard d'un nombre restreint de fournisseurs.

Le CCBE a déjà exprimé ses préoccupations concernant le CLOUD Act (loi sur la clarification de l'utilisation licite des données à l'étranger) des États-Unis, notamment en raison de sa compétence extraterritoriale, des conflits avec les droits fondamentaux de l'Union européenne et le RGPD, du caractère limité du contrôle juridictionnel, de l'absence de contrôle postérieur à l'autorisation et de la protection insuffisante du privilège juridique professionnel et du secret professionnel.[4]

Les sanctions imposées par les États-Unis à l'encontre de la Cour pénale internationale (CPI) illustrent la vulnérabilité des institutions judiciaires lorsque leur fonctionnement quotidien dépend de services fournis par des entités soumises à des obligations juridiques imposées par des pays tiers ou à des pressions géopolitiques. L'exemple de la CPI met en évidence un risque plus général pour la confidentialité et la continuité du service lorsque l'accès aux services de communication, de collaboration, de stockage ou de paiement dépend de prestataires soumis à des régimes de sanctions étrangers ou à des décisions politiques unilatérales.[5]

2. Remarques particulières

2.1 Application de la CADA aux barreaux et aux ordres d'avocats

Le CCBE constate que la formulation actuelle des dispositions proposées dans le cadre de la CADA pourrait être interprétée comme permettant leur application directe ou indirecte à certains barreaux ou ordres d'avocats, dans la mesure où ceux-ci fournissent des services d'informatique en nuage ou des services informatiques à leurs membres ou à un ensemble plus large de professionnels de la justice. Le CCBE estime qu'une telle interprétation présente un danger en raison du risque d'atteinte aux droits fondamentaux, notamment à l'indépendance de la représentation en justice et au privilège juridique professionnel, et, par conséquent, à l'État de droit.

Les barreaux et les ordres d'avocats ne sont pas des acteurs économiques ordinaires. En tant qu'organismes professionnels autonomes, ils ont pour mission de préserver l'indépendance de la profession d'avocat, de protéger le secret professionnel et de veiller à la bonne administration de la justice. L'application à ces institutions d'un régime de reconnaissance et de surveillance conçu pour des prestataires commerciaux risque de compromettre leur autonomie institutionnelle, qui constitue une pierre angulaire de l'État de droit et une condition préalable à la protection juridique effective des citoyens.

Concrètement, la reconnaissance au niveau d'assurance 1 nécessiterait une autoévaluation au titre de l'article 19, conformément à l'annexe I ; les niveaux d'assurance 2, 3 ou 4 entraîneraient en outre la réalisation d'audits indépendants au titre de l'article 20 ; et l'article 26 habiliterait les autorités nationales compétentes à inspecter les locaux de ces prestataires de services. Si le CCBE ne conteste

[4] Analyse du CCBE concernant le « CLOUD Act » des États-Unis (février 2019) : https://www.ccbe.eu/wp-content/uploads/2026/09/FR_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf

[5] Déclaration du CCBE concernant la CPI : https://www.ccbe.eu/wp-content/uploads/2026/09/FR_NA_20260722_CCBE-Statement-in-support-of-the-International-Criminal-Court-in-response-to-sanctions-imposed-by-the-US-administration.pdf

pas que les prestataires de services doivent démontrer à l'autorité de surveillance comment les données sont traitées et stockées, **il est essentiel que cette autorité n'ait pas accès aux données des avocats et des barreaux**. Il ne s'agit pas d'un simple détail technique, mais d'une question fondamentale touchant à l'indépendance des barreaux à l'égard de l'État, protégée par l'article 7 de la Charte des droits fondamentaux et par la jurisprudence relative au secret professionnel.

Le CCBE constate également que la situation des barreaux et les services qu'ils fournissent varient considérablement d'un ordre juridique à l'autre. Il est nécessaire de préciser si les barreaux doivent être considérés comme des prestataires, des exploitants ou de simples utilisateurs des infrastructures numériques de la justice, car leur rôle varie sensiblement selon les États membres, et toute obligation découlant de la CADA pourrait avoir des conséquences importantes sur les coûts, la gouvernance et l'indépendance de la profession. Les exemples suivants illustrent cette diversité.

En **Slovénie**, l'Ordre des avocats de Slovénie (OZS) procède actuellement à la modernisation de son progiciel de gestion intégré (ERP) et de son registre électronique des avocats, ce qui ouvrira de nouvelles possibilités d'interconnexion numérique de ce registre avec d'autres systèmes. Ainsi, en modernisant son registre et en le reliant aux systèmes de justice en ligne, le barreau pourrait devenir une source authentique ou un prestataire de services sur lequel s'appuient les pouvoirs publics.

Jusqu'à présent, le barreau a tenu le registre des avocats et a délivré leurs cartes professionnelles (articles 31 et 32, respectivement, de la loi slovène sur la profession d'avocat).[6] Ce registre est accessible au public sur le site internet du barreau et les juridictions s'y réfèrent pour vérifier la qualité professionnelle des avocats. Les assemblées régionales du barreau tiennent également des listes spécifiques d'avocats intervenant au titre de l'aide juridique gratuite et des désignations d'office, et le barreau publie les décisions disciplinaires prises à l'encontre des avocats.

En vertu de l'article 1er de cette loi, la profession d'avocat constitue un service autonome et indépendant faisant partie du système judiciaire.

En **Grèce**, les barreaux exploitent de vastes plateformes numériques utilisées par les avocats dans leurs relations avec les juridictions et les pouvoirs publics. Par l'intermédiaire de la plateforme exploitée sous l'égide de l'Assemblée plénière des barreaux grecs, les barreaux grecs proposent un large éventail de services électroniques, notamment le dépôt électronique, l'accès aux informations judiciaires ainsi que diverses fonctionnalités d'authentification et de certification.

En **Estonie**, le barreau estonien est principalement client et personne concernée au regard des infrastructures d'autres organismes, plutôt que prestataire de services. Il ne fournit pas de services d'informatique en nuage et n'exploite pas l'infrastructure permettant aux avocats de communiquer avec les juridictions : cette infrastructure (e-toimik, le système d'information des juridictions) est développée et exploitée par l'État. Le seul système d'information de l'État dans lequel le barreau exerce un rôle formel est le système d'information relatif à l'aide juridique de l'État (RIS), régi par le règlement du gouvernement n° 13 du 20 juin 2021.[7] Depuis le 1er janvier 2025, le ministère de la Justice et des Affaires numériques en est le responsable du traitement, tandis que le barreau estonien

[6] Zakon o odvetništvu (ZOdv) : https://pisrs.si/pregledPredpisa?id=ZAKO265

[7] Statuts du système d'information relatif à l'aide juridique de l'État, adoptés le 20 juin 2021, n° 13, RT I, 25 juin 2021, 19

et le Centre des registres et des systèmes d'information (RIK) en sont les sous-traitants. C'est le RIK, et non le barreau, qui est chargé de l'hébergement du système (§ 6, paragraphe 2, point 1).

Par ailleurs, certains barreaux modernisent régulièrement leurs services et envisagent de les développer, ce qui pourrait modifier leur nature et leur qualification au regard de la proposition de CADA.

Le CCBE est convaincu que la CADA ne devrait ni dissuader les barreaux de poursuivre ces évolutions ni les soumettre à des formes de surveillance étatique incompatibles avec l'indépendance de la profession et la protection du privilège juridique professionnel. Si le CCBE et ses membres reconnaissent pleinement la nécessité de maintenir un niveau élevé de maîtrise opérationnelle, de résilience, de sécurité et de protection contre les dépendances extérieures, ils estiment respectueusement que, pour garantir l'indépendance de la profession d'avocat, ces mesures gagnent à être mises en œuvre dans le cadre des dispositifs d'autorégulation existants des barreaux et des ordres d'avocats.

Si la Commission estime, dans certains cas, que les dispositions de la CADA doivent s'appliquer aux barreaux et aux ordres d'avocats, le CCBE insiste pour qu'une disposition expresse soit ajoutée afin de garantir que les pouvoirs d'inspection respectent l'indépendance des barreaux et ne s'étendent pas aux données couvertes par le secret professionnel et que, lorsque de telles données sont concernées, l'accès à celles-ci soit soumis à des garanties équivalentes à celles applicables aux perquisitions dans les cabinets d'avocats : autorisation judiciaire, désignation précise des données concernées et intervention du barreau compétent.

Les recherches menées par le CCBE dans neuf ordres juridiques de l'Union européenne montrent que, dans chacun d'eux, les perquisitions dans les cabinets d'avocats doivent reposer sur une base légale formelle, prenant presque toujours la forme d'un mandat judiciaire ou d'une décision judiciaire motivée.[8] Par exemple :

- En **Belgique**, les perquisitions domiciliaires et dans les locaux professionnels, y compris lorsqu'elles portent sur les systèmes informatiques, nécessitent un mandat délivré par un juge d'instruction, sauf en cas de consentement ou de flagrant délit, situations dans lesquelles le procureur du Roi peut intervenir.[9]
- En **France,** les perquisitions au cabinet ou au domicile d'un avocat nécessitent une décision écrite et motivée rendue par un magistrat, à savoir le juge des libertés et de la détention, précisant l'infraction concernée, l'objet de la perquisition et sa proportionnalité au regard de la nature de l'infraction (article 56-1 du Code de procédure pénale).
- En **Allemagne,** les perquisitions doivent être ordonnées par un juge en vertu du § 105 du Code de procédure pénale allemand (*Strafprozeßordnung* – StPO)[10], sous réserve d'exceptions limitées en cas d'urgence, dans lesquelles le ministère public peut intervenir.

[8] Belgique, France, Allemagne, Grèce, Irlande, Italie, Lettonie, Pays-Bas et Slovénie.

[9] Référence légale : article 39bis, § 9, du Code d'instruction criminelle : https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=fr&sum_date=&pd_search=1808-11-27&numac_search=1808111701&page=1&lg_txt=F&caller=list&1808111701=7&trier=promulgation&view_numac=2022b30600fx1804032130fr&dt=CODE+D%27INSTRUCTION+CRIMINELLE&fr=f&choix1=ET#LNK0010

[10] Version anglaise : https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

- En **Italie,** les perquisitions dans les cabinets d'avocats doivent être effectuées personnellement par un juge ou, au cours de l'enquête préliminaire, par le ministère public agissant sur la base d'une autorisation judiciaire motivée, conformément à l'article 103 du Code de procédure pénale italien (*Codice di procedura penale*, CPP).[11]
- En **Slovénie,** une perquisition dans un cabinet d'avocats ne peut être effectuée que sur la base d'un mandat de perquisition délivré par une juridiction, quel que soit le domaine du droit concerné.
- En **Irlande**, les mandats de perquisition sont délivrés par les juges des District Courts ou par les peace commissioners (commissaires de paix), sur la base d'informations fournies sous serment par la police.

En outre, dans de nombreux ordres juridiques, l'exécution d'un mandat de perquisition dans un cabinet d'avocats est soumise à des garanties procédurales destinées à protéger le secret professionnel ou *legal professional privilege* ou le secret professionnel. La première de ces garanties supplémentaires réside dans la présence du bâtonnier, ou de son représentant, lors des perquisitions dans les cabinets d'avocats (par exemple en Belgique, en France, en Italie, en Lettonie, aux Pays-Bas et en Slovénie). La deuxième garantie supplémentaire réside dans le traitement particulier réservé aux informations détenues par un avocat ou un cabinet d'avocats. Elle comprend notamment des dispositions spécifiques définissant les informations qui doivent être exclues du champ des perquisitions ou des éléments de preuve susceptibles d'être utilisés ultérieurement au cours de la procédure.

2.2 Méthodologie d'évaluation des risques au titre de l'article 29

Le CCBE estime important que les résultats de l'évaluation des risques prévue à l'article 29 permettent une interprétation cohérente du niveau de risque et du niveau d'assurance à appliquer à un même secteur ou à des activités identiques. Cela revêt une importance particulière dans un contexte marqué par la multiplication des procédures judiciaires et des mesures d'enquête transfrontalières, ainsi que par les initiatives au niveau de l'Union visant à encourager l'adoption de l'intelligence artificielle et d'autres technologies numériques par le système judiciaire.[12]

Le CCBE propose que la méthodologie devant être adoptée par la Commission en vertu de l'article 29, paragraphe 3, impose la consultation des barreaux lors de l'évaluation des activités du secteur judiciaire dont les avocats et les barreaux sont utilisateurs ou pour lesquelles ils pourraient être considérés comme des prestataires. La méthodologie d'évaluation des risques devrait également intégrer la nécessité d'assurer le niveau de protection le plus élevé aux informations couvertes par le secret professionnel. L'exemple du système d'information des juridictions estoniennes illustre l'importance d'une telle consultation. Ses utilisateurs comprennent non seulement les avocats et le personnel du barreau, mais également le personnel habilité des juridictions, du parquet et des autorités d'enquête (§ 7, paragraphe 1), dès lors que l'autorité chargée de la procédure détermine les honoraires sur la base des informations enregistrées dans le système. La classe de sécurité et le niveau

[11] Version anglaise : https://canestrinilex.com/assets/Uploads/pdf/cf70b10e21/Italian-Code-of-Criminal-Procedure-canestriniLex.pdf

[12] Stratégie DigitalJustice@2030 : https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/digitalisation-justice/communication-digitaljustice2030_en

de sécurité du système ont été définis par voie réglementaire. Dans le cadre de la CADA, ce même système serait évalué par l'État membre concerné en tant qu'activité relevant du secteur judiciaire au titre de l'article 29, selon une méthodologie établie par un acte d'exécution de la Commission. **Selon le CCBE, cette méthodologie devrait imposer la consultation de la profession d'avocat.**

Par ailleurs, certains barreaux peuvent être des prestataires de services de confiance qualifiés au sens du règlement eIDAS. Ainsi, le Conseil général du barreau espagnol (CGAE) est un prestataire de services de confiance qualifié par l'intermédiaire de son autorité de certification (ACA), statut qui figure également sur la liste de confiance espagnole, et il délivre des certificats électroniques qualifiés aux avocats. Le CGAE assure l'identification et l'authentification électroniques des avocats (ACA et ACA Plus, ainsi que le système d'accès unique du barreau espagnol, également proposé aux barreaux locaux pour l'identification de leurs membres), des services liés à l'aide juridique ainsi que l'échange du registre national des avocats avec le ministère de la Justice et avec la Generalitat de Catalunya. Le CGAE prévoit de poursuivre le développement de certificats qualifiés reposant sur l'informatique en nuage au cours de la deuxième phase de mise en œuvre d'ACA Plus. Par souci d'exactitude, il convient de préciser que le CGAE n'exploite pas la plateforme permettant aux avocats de communiquer avec les juridictions : en Espagne, les avocats accèdent à LexNET, exploité par le ministère de la Justice, ou aux systèmes équivalents des communautés autonomes, soit directement, soit par l'intermédiaire de leurs propres logiciels de gestion des dossiers.

3. Remarques finales

Le CCBE invite également la Commission et les autres parties prenantes à réfléchir à la diversité du marché européen des services informatiques et aux conséquences de la situation actuelle pour les ordres juridiques de plus petite taille. Des dispositions strictes risquent de réduire le nombre de prestataires satisfaisant aux niveaux d'assurance requis et, par conséquent, de priver le marché d'offres concurrentielles, dès lors que, dans les marchés de taille réduite, les réglementations imposant des exigences plus élevées sont souvent adoptées avant même que les services correspondants soient disponibles sur le marché. En outre, pour certains barreaux, notamment ceux des ordres juridiques de plus petite taille, les obligations supplémentaires liées à la surveillance ou au contrôle du respect d'exigences plus strictes constitueraient une charge supplémentaire.

Le CCBE invite par ailleurs la Commission à envisager la reconnaissance des cadres nationaux équivalents plutôt que d'exiger leur reformulation. Certains États membres disposent déjà d'un régime d'assurance opérationnel, obligatoire et applicable à l'échelle nationale, couvrant les systèmes utilisés dans le secteur judiciaire, qui est adopté et appliqué système par système plutôt que prestataire par prestataire, et qui n'est pas exprimé en niveaux d'assurance de l'Union.