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 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)

Introduction et résumé

Le Conseil des barreaux européens (CCBE) représente les barreaux de 46 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.

Le 23 février 2022, la Commission européenne a présenté une proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données). Elle vise à garantir l'équité dans la répartition de la valeur des données entre les acteurs de l'économie des données et à favoriser l'accès aux données ainsi que leur utilisation.

Après son analyse de la proposition, le CCBE arrive aux conclusions suivantes :

- **Le champ d'application personnel et matériel de la proposition de règlement sur les données est trop large.**
- **Le règlement sur les données devrait prévoir une disposition générale pour assurer une protection adéquate des PS/LPP. Par conséquent :**
  - **Le considérant (7) devrait être modifié pour indiquer que le règlement ne doit pas porter préjudice au secret professionnel en vertu du droit national, comme les règles sur la protection des communications professionnelles entre les avocats et leurs clients.**
  - **L'article 1 devrait être modifié pour inclure un paragraphe 5 stipulant que le règlement n'affecte pas les règles nationales sur la protection du secret professionnel. Les obligations prévues par le présent règlement ne devraient pas s'appliquer aux professionnels soumis au secret professionnel, tel que prévu par le droit national, lorsque ces obligations conduiraient ces professionnels à violer leur secret professionnel.**
- **Le champ d'application et les conditions de mise à disposition des données aux organismes publics devraient être clarifiés. L'absence de définition claire des notions de "*besoin exceptionnel*" et d'"*urgence publique*", et la référence aux procédures nationales créent un risque élevé d'interprétations divergentes des concepts concernés et augmentent la probabilité d'interférence avec les droits fondamentaux. La proposition devrait délimiter plus clairement le type de situations qui constitueraient une urgence publique.**
- **La justification d'une demande de données devrait être mieux définie dans la proposition. Les circonstances justificatives telles que l'incapacité d'adopter des mesures législatives à temps, ainsi que la réduction de la charge administrative, devraient être retirées de la proposition.**

- **La proposition devrait exclure la possibilité pour les organismes publics de demander des données couvertes par un secret professionnel, ainsi que l'obligation pour les détenteurs de données de divulguer ces données.**
- **Les institutions de l'UE et les fournisseurs de services en nuage doivent prendre des mesures afin de s'assurer que des mesures techniques, juridiques et organisationnelles raisonnables sont en place pour empêcher l'accès non autorisé à des données couvertes par le secret professionnel ou le secret professionnel légal.**
- **Les obligations de l'article 30 ne sont pas suffisamment justifiées et ne respectent pas le principe de neutralité technologique. Ces dispositions devraient être supprimées de la proposition.**

Commentaires généraux

Le CCBE constate que la proposition de règlement sur les données a un champ d'application très large, qu'elle couvre de nombreuses situations et destinataires qui ne sont pas nécessairement liés et comprend des règles poursuivant des objectifs différents. En effet, la proposition prévoit des règles sur le droit des utilisateurs d'accéder et d'utiliser les données générées par l'utilisation de produits ou de services liés (articles 3 et suivants) ; sur les clauses contractuelles abusives (article 13) ; sur la disponibilité des données pour le secteur public (articles 14-22) ; sur les services de traitement des données, qui sont plus communément considérés comme des fournisseurs de services en nuage (articles 23-26), le transfert à l'échelle internationale de données à caractère non personnel (article 27), l'interopérabilité (articles 28-29) et les contrats intelligents (30).

En particulier, l'obligation de rendre les données accessibles (article 3, paragraphe 1) ou de les mettre à disposition (article 4, paragraphe 1) peut s'appliquer à presque tout le monde étant donné qu'il n'y a pratiquement aucune délimitation du cercle des détenteurs de données, des produits, des services liés ou de la nature des données. Les définitions de l'article 2 à cet égard sont excessivement larges. De plus, l'application des obligations relatives aux produits et services liés aux assistants virtuels, conformément à l'article 7, paragraphe 2, élargit encore le champ d'application et suggère, par rapport à la définition du service lié à l'article 2, paragraphe 3, une conception large du lien entre le service et le produit, qui n'est plus que vaguement lié à la nécessité d'exploiter le produit.

Le CCBE considère que le champ d'application personnel et matériel de la proposition de règlement sur les données est trop large (Art. 1 §§1-2).

I. La nécessité de garantir le secret professionnel

A. Une protection renforcée du secret professionnel

Le CCBE rappelle que pour que les avocats soient efficaces dans la défense des droits de leurs clients, il doit y avoir une confiance dans la confidentialité de leurs communications. La plupart des systèmes juridiques partagent une compréhension commune du fait que si le droit du citoyen à la préservation de la confidentialité, c'est-à-dire le droit du citoyen à être protégé contre toute divulgation de ses communications avec son avocat, devait être refusé, les personnes pourraient se voir refuser l'accès aux conseils juridiques et à la justice. Le secret professionnel est donc considéré comme un instrument permettant l'accès à la justice et le maintien de l'état de droit.

Tous les pays européens ont des dispositions nationales afin d'assurer la protection du droit et du devoir des avocats de préserver la confidentialité des affaires de leurs clients. Dans certaines juridictions, ce but est atteint en offrant à ces communications la protection du *legal professional privilege* et, dans d'autres, en les traitant comme relevant du secret professionnel. Les deux approches cherchent cependant à atteindre le même objectif : la protection des informations générées dans le cadre de la relation avocat-client dans le but de donner ou de recevoir des conseils juridiques, dans les domaines contentieux et non contentieux, ou la représentation dans tout type de procédure judiciaire. Cette obligation absolue de confidentialité incombe directement à l'avocat et le client ne peut pas y renoncer dans la plupart des juridictions. Dans certains États membres, le secret professionnel a un statut constitutionnel visant à garantir les droits fondamentaux tels que le droit à la vie privée ou le droit à un procès équitable. Dans certaines juridictions, la violation du secret professionnel par les avocats, telle que la divulgation de données concernées, constitue une infraction pénale.

La Cour européenne des droits de l'homme a, à plusieurs reprises, lié le respect des relations entre avocats et clients au respect des **articles 6 et 8 de la Convention européenne des droits de l'homme**, en déclarant que « *le respect du droit du justiciable à un procès équitable »*[1] *dépend de la « relation de confiance entre [l'avocat et son client]* » et en soulignant à plusieurs reprises que l'atteinte aux relations entre avocats et clients peut violer l'article 8, qui protège le droit au respect de la vie privée et familiale. En effet, l'**article 8 « *accorde une protection renforcée aux échanges entre les avocats et leurs clients* »**. La Cour précise : « *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* »[2].

La protection de la confidentialité des communications entre un avocat et son client a également été reconnue comme un **principe général du droit de l'UE** par la Cour européenne de justice[3] et a une **base juridique dans la Charte des droits fondamentaux de l'UE dans ses articles 7 sur le droit à la vie privée et 47 sur le droit à un procès équitable**.

B. Le règlement sur les données et le secret professionnel

La proposition de règlement sur les données prévoit plusieurs obligations de mise à disposition des données. Le CCBE note que le considérant (7) de la proposition de règlement sur les données prévoit qu'« *Aucune disposition du présent règlement ne devrait être appliquée ou interprétée de manière à réduire ou à limiter le droit à la protection des données à caractère personnel ou le droit à la vie privée et à la confidentialité des communications* », avec une référence spécifique au RGPD[4] et à la directive vie privée et communications électroniques[5]. Elle comporte également des dispositions visant à garantir le respect des secrets commerciaux ou des droits de propriété intellectuelle. Le CCBE salue ces dispositions mais les considère comme insuffisantes pour assurer la protection du secret professionnel telle que garantie par la CEDH et le droit primaire de l'UE étant donné que ce principe peut concerner des données qui ne sont ni à caractère personnel ni protégées par des secrets commerciaux.

Le CCBE rappelle que lorsque le législateur européen a adopté des dispositions transitoires pour modifier la directive vie privée et communications électroniques afin de l'adapter à la lutte contre les abus sur les

[1] CEDH, Michaud c. France (12323/11), 2012, §§117-118
[2] CEDH, Kopp c. Suisse (23224/94), 1998
[3] CJCE, AM&S c. Commission, (155/79), 1982, §18
[4] Règlement (UE) 2016/679
[5] Directive 2002/58/CE

enfants, il a explicitement prévu une clause générale sur la protection du secret professionnel, précisant que les nouvelles règles devaient être « ***sans préjudice des règles relatives au secret professionnel prévues par le droit national, telles que les règles relatives à la protection des communications professionnelles entre les médecins et leurs patients, entre les journalistes et leurs sources, ou entre les avocats et leurs clients, en particulier puisque la confidentialité des communications entre les avocats et leurs clients est capitale pour garantir l'exercice effectif des droits de la défense, qui constituent un élément essentiel du droit à un procès équitable*** ».

Le CCBE considère que le règlement sur les données devrait prévoir une disposition générale pour assurer une protection adéquate du secret professionnel. Par conséquent :

- **Le considérant (7) devrait être modifié pour indiquer *in fine* que le règlement ne devrait pas porter préjudice au secret professionnel en vertu du droit national, comme les règles sur la protection des communications professionnelles entre les avocats et leurs clients.**
- **L'article 1 devrait être modifié pour inclure un paragraphe 5 indiquant que le règlement n'affecte pas les règles nationales sur la protection du secret professionnel. Les obligations prévues par le présent règlement ne devraient pas s'appliquer aux professionnels tenus au secret professionnel, tel que prévu par le droit national, lorsque ces obligations conduiraient ces professionnels à violer leur secret professionnel.**

II. Obligation de mettre les données à la disposition des organismes du secteur public et des institutions, organes ou organismes de l'Union en cas de « besoin exceptionnel »

L'article 14(1) de la proposition de règlement sur les données prévoit l'obligation pour les détenteurs de données de mettre les données à la disposition des autorités publiques, des institutions, organes et organismes de l'UE en cas de « *besoin exceptionnel* ». Le CCBE constate que cet accès est encadré par les articles 15, 16, 17 et suivants. Le champ d'application des besoins exceptionnels est défini à l'article 15 comme la nécessité de réagir à une urgence publique, et l'article 16 exclut les activités menées à des fins de prévention et de détection des infractions pénales ou administratives, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales, ou d'administration douanière ou fiscale. L'article 17 contient les conditions auxquelles doivent répondre les demandes.

Néanmoins, le CCBE exprime de profondes inquiétudes quant à ces demandes de données par les organismes publics. Comme le soulignent le Comité européen de la protection des données (« l'EDPB ») et le Contrôleur européen de la protection des données (« le CEPD ») « ***les principes de nécessité et de proportionnalité, la base juridique doit également définir l'étendue et les modalités de l'exercice de leurs pouvoirs par les autorités compétentes et être assortie de garanties suffisantes pour protéger les personnes contre toute ingérence arbitraire*** » ; à cet égard, l'EDPB et le CEPD « ***observent que les circonstances justifiant l'accès ne sont pas étroitement spécifiées et estiment nécessaire que le législateur définisse de manière beaucoup plus stricte les hypothèses d'urgence ou de besoin exceptionnel*** »[6].

Le CCBE considère que les dispositions générales sur les demandes de données des organismes publics créent un risque d'abus, malgré les conditions de la proposition prévoyant que (a) cette obligation de mettre les données à la disposition des organismes publics n'affectera pas les données à caractère personnel et (b) que ces données ne peuvent pas être utilisées à des fins de prévention et de détection des infractions pénales ou

[6] Avis conjoint EDPB-CEPD 02/2022 sur la proposition du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), 4 mai 2022, p.3.

administratives, d'enquêtes et de poursuites en la matière, d'exécution de sanctions pénales, ou d'administration douanière ou fiscale, etc. L'histoire a démontré à maintes reprises qu'il est très difficile de faire respecter ces interdictions. La différence entre les données à caractère non personnel et les données à caractère personnel est très vague, même après des années d'expérience commune du GDPR, et plus on a accès à des données non personnelles, plus il est facile d'identifier ou de réduire d'une autre manière le champ possible des personnes concernées. Il ne fait aucun doute qu'il y aura certainement des organismes publics qui céderont à cette tentation d'accès facile à de si vastes mines de données, la question étant plutôt de savoir comment il sera possible de le découvrir.

Le CCBE estime dès lors que le champ d'application et les conditions de mise à disposition des données aux organismes publics devraient être clarifiés.

En ce qui concerne les justifications d'une demande de données par les organismes publics, la proposition exige la démonstration d'un « besoin exceptionnel ». Selon l'article 15, ce « besoin exceptionnel » est lié à la nécessité de réagir à une urgence publique, de prévenir une urgence publique ou de s'en rétablir, ou d'accomplir une mission d'intérêt public prévue par la loi. La notion d'« urgence publique » est largement définie à l'article 2, paragraphe 10, comme « *une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou les États membres concernés*». Il convient de noter que le considérant (57) donne des exemples d'urgences publiques, telles que les urgences de santé publique, celles résultant de la dégradation de l'environnement, les catastrophes majeures d'origine naturelle ou humaine. Le considérant fait *in fine* référence aux urgences publiques déterminées selon les procédures respectives des États membres ou des organisations internationales.

Le CCBE considère que l'absence de définition claire des concepts de « besoin exceptionnel », d'« urgence publique » et la référence aux procédures nationales créent un risque élevé d'interprétations divergentes des concepts concernés et augmentent la probabilité d'atteinte aux droits fondamentaux. Le CCBE soutient les recommandations de l'EDPB et du CEPD de modifier la proposition afin de délimiter plus clairement le type de situations qui constitueraient une urgence publique[7].

En outre, le CCBE a des préoccupations similaires concernant la justification d'une demande de données lorsque le manque de données disponibles empêche l'autorité publique de remplir une mission spécifique dans un intérêt public explicitement prévu par la loi. Pour cette justification, l'article 15(c) fait référence à deux situations : (1) lorsque l'autorité publique n'a pas été en mesure d'obtenir les données par d'autres moyens, y compris lorsque des mesures législatives ne peuvent être adoptées à temps pour rendre les données disponibles, ou (2) lorsque l'obtention des données réduirait substantiellement la charge administrative.

À cet égard, le CCBE soutient les conclusions des autorités européennes de protection des données[8] et considère que :

- **La possibilité de demander des données, lorsque des mesures législatives ne peuvent être adoptées à temps, va à l'encontre des conditions de l'article 52(1) de la Charte des droits fondamentaux de l'UE selon lequel toute limitation des droits fondamentaux doit être prévue par la loi.**
- **La réduction de la charge administrative ne peut constituer une justification suffisante d'atteinte aux droits fondamentaux.**

De telles circonstances devraient être retirées de la proposition, qui devrait mieux définir la justification d'une demande de données.

[7] Avis conjoint EDPB-EDPS 02/2022, §78

[8] Avis conjoint EDPB-EDPS 02/2022, §79

Enfin, alors que les articles 17, paragraphe 2 point c), 18, paragraphe 5, et 19, paragraphe 2 contiennent des dispositions visant à protéger les secrets commerciaux, **la proposition n'offre aucune protection du secret professionnel des personnes concernées.**

Tel qu'évoqué ci-dessus, la proposition devrait exclure la possibilité pour les organismes publics de demander des données relevant du professionnel, ainsi que l'obligation pour les détenteurs de données de divulguer celles-ci.

III. Exigences concernant l'utilisation des services en nuage

Le règlement sur les données contient des dispositions assez détaillées relatives aux fournisseurs de services de traitement des données, plus communément appelés fournisseurs de services en nuage, visant à aider les utilisateurs de services en nuage à changer de fournisseur de services (articles 23 à 26, et article 29). En outre, les fournisseurs de services en nuage non-PME doivent « *prennent toute les mesures techniques, juridiques et organisationnelles raisonnables* » afin d'empêcher le transfert à l'échelle internationale de données non personnelles ou l'accès de gouvernements tiers à celles-ci (article 27.1).

Le CCBE fait remarquer qu'au cours des dernières années, les services d'informatique en nuage ont considérablement mûri. Les processus de sécurité sont devenus plus robustes avec des attestations de tiers largement acceptées et des garanties quant à la fiabilité des contrôles de sécurité informatique. Certains contrôles de sécurité informatique font toutefois encore défaut. **Tant que le fournisseur de services (ou toute plateforme ou infrastructure sous-jacente) est techniquement capable de lire et d'accéder aux données de l'avocat, les risques d'accès non autorisé, et donc de violation de la confidentialité et des obligations liées au secret professionnel, resteront une préoccupation grave pour les avocats**. Des préoccupations similaires découlent de la réutilisation des données des clients à d'autres fins ou de l'interception illégale des communications par les autorités[9].

Le CCBE travaille actuellement sur l'utilisation des services en nuage par les avocats en Europe. L'objectif global de cette action est d'adapter le secret professionnel à l'ère numérique en définissant des mécanismes de défense contre l'accès non autorisé aux informations relevant du secret professionnel.

À cet égard, le CCBE appelle les institutions de l'UE et les fournisseurs de services en nuage à prendre des mesures afin de s'assurer que des mesures techniques, juridiques et organisationnelles raisonnables sont en place pour empêcher tout accès non autorisé à des données protégées par le secret professionnel.

IV. Exigences essentielles des contrats intelligents

L'article 30 indique que les vendeurs d'une application utilisant des contrats intelligents sont tenus de se conformer aux exigences essentielles énumérées, telles que la robustesse, la résiliation en toute sécurité, etc., qui serviront de base à une déclaration de conformité et dont les détails seront définis ultérieurement par des normes. Le CCBE tient à préciser que, dans sa forme actuelle, sans aucune mesure provisoire, l'article 30 constitue une approche dangereuse, inutilement précipitée.

[9] Guide sur l'utilisation des outils reposant sur l'intelligence artificielle par les avocats et les cabinets d'avocats dans l'UE, 2022, p. 47,48 et 51.

Le CCBE est fermement convaincu qu'indépendamment des moyens techniques utilisés, la protection des consommateurs et toute autre obligation juridique fixée par la loi doivent être maintenues par toutes les parties.

La déclaration de conformité est un outil approprié pour les marchés mûrs disposant de normes existantes sur, par exemple, la sécurité ou d'autres exigences, libérant l'organisme de réglementation, entre autres, de la charge de devoir mettre à jour fréquemment les exigences législatives. Mais il n'a jamais été prévu de l'utiliser pour externaliser la charge réglementaire à des acteurs du marché plus importants disposant des ressources nécessaires pour envoyer des experts dans les organismes de normalisation de l'UE, tels que l'Institut européen de normalisation des télécommunications (ETSI).

Personne ne s'attend vraiment à recevoir des orientations ou des normes dans les années à venir sur la manière dont les exigences essentielles définies dans la proposition de règlement sur les données pourraient être mises en œuvre dans les registres distribués. Il n'y a aucune mesure transitoire ou de mise en œuvre faisant référence aux contrats intelligents dans la proposition de règlement sur les données, et ces questions n'ont pas été étudiées dans l'analyse d'impact. Il s'agit davantage d'un problème de sécurité juridique et de pertinence de l'approche réglementaire envisagée, que d'un problème direct pour les avocats, mais les entreprises en Europe se tourneront probablement vers leurs avocats dans l'UE pour obtenir des conseils sur ces questions et, en raison des dispositions actuelles, les avocats ne seront pas en mesure de fournir de tels conseils.

Le CCBE estime par conséquent que les obligations étendues de l'article 30 ne sont pas suffisamment justifiées et ne respectent pas le principe de neutralité technologique. Ces dispositions devraient être supprimées de la proposition.