EUROPEAN LAWYERS
EUROPEAN BARS CCBE BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

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

Posicionamiento de CCBE sobre la propuesta de Reglamento sobre normas armonizadas para el acceso y el uso equitativo de los datos (Ley de datos)

Introducción y resumen

El Consejo de la Abogacía Europea (CCBE) representa a los colegios de abogados de 46 países y, a través de ellos, a más de un millón de abogados europeos. El CCBE responde regularmente en nombre de sus miembros sobre cuestiones políticas que afectan a los ciudadanos y abogados europeos.

El 23 de febrero de 2022, la Comisión Europea presentó una propuesta de Reglamento sobre normas armonizadas para un acceso y uso justos de los datos (Ley de Datos). Su objetivo es garantizar la equidad en la asignación del valor de los datos entre los agentes de la economía de los datos y fomentar el acceso a los datos y su uso.

Tras su análisis de la propuesta, el CCBE concluye:

- **El ámbito personal y material de la propuesta de Ley de Datos es demasiado amplio.**
- **La Ley de Datos debe prever una disposición general que garantice una protecciónadecuada de los PS/LPP. Por lo tanto:**
    - **Los considerandos (7) deben modificarse para incluir que el Reglamento debe entenderse sin perjuicio del secreto profesional en virtud de la legislación nacional, como las normas sobre protección de las comunicaciones profesionales entre abogados y sus clientes.**
    - **El artículo 1 debe modificarse para incluir un apartado 5 que establezca que el Reglamento no afectará a las normas nacionales sobre protección del secreto profesional. Las obligaciones previstas por el presente Reglamento no deben aplicarse a los profesionales sujetos al secreto profesional, según lo dispuesto por la legislación nacional, cuando dichas obligaciones lleven a estos profesionales a violar su secreto profesional.**
- **Deben aclararse el alcance y las condiciones para poner los datos a disposición de los organismos públicos. La falta de una definición clara de los conceptos de "*necesidad excepcional*", "*emergencia pública*" y la referencia a los procedimientos nacionales crea un alto riesgo de interpretaciones divergentes de los conceptos implicados y aumenta la probabilidad de interferencia con los derechos fundamentales. La propuesta debería delimitar más claramente los tipos de situaciones que constituirían una emergencia pública.**
- **La justificación de una solicitud de datos debería definirse mejor en la propuesta. Deberían retirarse de la propuesta circunstancias justificativas como la imposibilidad de adoptar medidas legislativas a tiempo, así como la reducción de las cargas administrativas.**

- **La propuesta debe excluir la posibilidad de que los organismos públicos soliciten datos amparados por el secreto profesional, así como la obligación de que los titulares de los datos los revelen.**

- **Las instituciones de la UE y los proveedores de servicios en nube deben tomar medidas para garantizar que se aplican medidas técnicas, jurídicas y organizativas razonables para impedir el acceso no autorizado a datos amparados por el secreto profesional o la prerrogativa del secreto profesional.**

- **Las obligaciones del artículo 30 no están suficientemente justificadas y no respetan el principio de neutralidad tecnológica. Estas disposiciones deben eliminarse de la propuesta.**

Observaciones generales

El CCBE observa que la propuesta de Ley de Datos tiene un ámbito de aplicación amplio, que abarca muchas situaciones y destinatarios que no están necesariamente relacionados, y que contiene normas que persiguen objetivos diferentes. En efecto, la propuesta prevé normas sobre el derecho de los usuarios a acceder y utilizar los datos generados por el uso de productos o servicios relacionados (artículos 3 y siguientes); sobre las cláusulas contractuales abusivas (artículo 13); sobre la disponibilidad de datos para el sector público (artículos 14-22); sobre los servicios de tratamiento de datos, que más comúnmente se consideran proveedores de servicios en la nube (artículos 23-26), la transferencia internacional de datos no personales (artículo 27), la interoperabilidad (artículos 28-29) y los contratos inteligentes (30).

En particular, la obligación de hacer accesibles los datos (apartado 1 del artículo 3) o de ponerlos a disposición (apartado 1 del artículo 4) puede aplicarse a casi cualquiera, ya que apenas se delimita el círculo de los titulares de los datos, los productos, los servicios relacionados o la naturaleza de los datos. Las definiciones del artículo 2 a este respecto son excesivamente amplias. Asimismo, la aplicación de las obligaciones sobre productos y servicios relacionados a los asistentes virtuales, de conformidad con el apartado 2 del artículo 7, amplía aún más el ámbito de aplicación y sugiere, en relación con la definición de servicio relacionado del apartado 3 del artículo 2, una concepción amplia del vínculo entre el servicio y el producto, que ahora sólo se vincula vagamente a la necesidad de explotar el producto.

El CCBE considera que el ámbito de aplicación personal y material de la propuesta de Ley de datos es demasiado amplio (Art. 1 §§1-2).

I. La necesidad de garantizar secreto profesional / privilegio legal profesional ("SP/PLP")

A. Una protección reforzada de PS/ LPP

El CCBE recuerda que para que los abogados sean eficaces en la defensa de los derechos de sus clientes, debe existir la confianza de que las comunicaciones entre ellos se mantienen confidenciales. La mayoría de los sistemas jurídicos comparten la idea de que, si se negara el derecho del ciudadano a salvaguardar la confidencialidad, es decir, el derecho del ciudadano a ser protegido contra cualquier divulgación de su comunicación con su abogado se podría negar a las personas el acceso al asesoramiento jurídico y a la justicia. Así pues, los PS/LPP se consideran instrumentos mediante los cuales se puede lograr el acceso a la justicia y el mantenimiento del Estado de Derecho.

Todos los países europeos cuentan con disposiciones nacionales para garantizar la protección del derecho y el deber de los abogados de mantener la confidencialidad de los asuntos de los clientes. En algunas jurisdicciones, esto se consigue otorgando a esas comunicaciones la protección del secreto profesional de los abogados, y en otras jurisdicciones tratándolas como secretos profesionales. Sin embargo, ambos enfoques persiguen el mismo fin: la protección de la información, generada dentro de la relación abogado-cliente con el fin de dar o recibir asesoramiento jurídico, tanto en asuntos contenciosos como no contenciosos, y/o representación en cualquier tipo de procedimiento judicial. Esta obligación absoluta de confidencialidad recae directamente sobre el abogado y no puede ser renunciada por el cliente en la mayoría de las jurisdicciones. En algunos Estados miembros, el secreto profesional tiene rango constitucional para garantizar derechos fundamentales como el derecho a la intimidad o el derecho a un juicio justo. En algunas jurisdicciones, la violación del secreto profesional por parte de los abogados, como la revelación de datos cubiertos, constituye un delito penal.

El Tribunal Europeo de Derechos Humanos ("TEDH") ha vinculado reiteradamente el respeto de la PS/LPP a la observancia de **los artículos 6 y 8 del Convenio Europeo de Derechos Humanos** ("CEDH"), afirmando que "*el derecho de toda persona a un proceso equitativo"*[1] *depende de la "relación de confianza entre [el abogado y el cliente]*" y subrayando repetidamente que socavar la PS/LPP puede violar el artículo 8, que protege el derecho al respeto de la vida privada y familiar. En efecto, **el artículo 8 "*otorga una protección reforzada a los intercambios entre los abogados y sus clientes*"**. El Tribunal precisa que "*esto se justifica por el hecho de que los abogados tienen asignado un papel fundamental en una sociedad democrática, el de defender a los justiciables. Ahora bien, no pueden desempeñar esta misión esencial si no pueden garantizar a sus defendidos la* confidencialidad de *sus intercambios". .*[2]

La protección de la confidencialidad de las comunicaciones entre abogado y cliente también ha sido reconocida como **principio general del Derecho de la UE** por el Tribunal de Justicia de las Comunidades Europeas[3] y tiene una **base jurídica en la Carta de los Derechos Fundamentales de la UE, en sus artículos 7 sobre el derecho a la intimidad y 47 sobre el derecho a un juicio justo**.

[1] ECtHR, Michaud v. France (12323/11), 2012, §§117-118
[2] TEDH, Kopp contra Suiza (23224/94), 1998
[3] TJCE, AM&S contra Comisión, (155/79), 1982, §18

B. Ley de protección de datos y PS/ LPP

La propuesta de Ley de Datos establece varias obligaciones de puesta a disposición de los datos. El CCBE señala que el considerando (7) de la propuesta de Ley de Datos establece que "*ninguna disposición del presente Reglamento debe aplicarse o interpretarse de manera que disminuya o limite el derecho a la protección de los datos personales o el derecho a la privacidad y confidencialidad de las comunicaciones*", con referencias específicas al GDPR[4]y a la Directiva sobre la privacidad y las comunicaciones electrónicas[5]. También contiene disposiciones para garantizar el respeto de los secretos comerciales o los derechos de propiedad intelectual. El CCBE acoge favorablemente dichas disposiciones, pero las considera insuficientes para garantizar la protección de los PS/PL, tal como garantizan el CEDH y el Derecho primario de la UE, ya que dicho principio puede abarcar datos que no son personales ni están protegidos por secretos comerciales.

El CCBE recuerda que cuando el legislador europeo adoptó las disposiciones transitorias para modificar la Directiva sobre la privacidad y las comunicaciones electrónicas con el fin de adaptarla a la lucha contra el abuso de menores, previó explícitamente una cláusula general sobre la protección de los PS/LPP, aclarando que las nuevas normas debían entenderse "***sin perjuicio de las normas sobre el secreto profesional previstas en el Derecho nacional", como las normas sobre protección de las comunicaciones profesionales, entre médicos y sus pacientes, entre periodistas y sus fuentes, o entre abogados y sus clientes, en particular porque la confidencialidad de las comunicaciones entre abogados y sus clientes es clave para garantizar el ejercicio efectivo de los derechos de la defensa como parte esencial del derecho a un juicio justo***".

El CCBE considera que la Ley de Datos debe prever una disposición general que garantice una protecciónadecuada de los PS/LPP. Por consiguiente:

-Los considerandos (7) deben modificarse para incluir in fine que el Reglamento debe entenderse sin perjuicio sobre el secreto profesional con arreglo a la legislación nacional, como las normas sobre la protección de las comunicaciones profesionales entre los abogados y sus clientes.

- El artículo 1 debe modificarse para incluir un apartado 5 que establezca que el Reglamento no afectará a las normas nacionales sobre la protección del secreto profesional. Las obligaciones previstas por el presente Reglamento no deben aplicarse a los profesionales sujetos al secreto profesional, según lo dispuesto por el Derecho nacional, cuando tales obligaciones puedan llevar a estos profesionales a violar su secreto profesional.

[4] Reglamento (UE) 2016/679
[5] Directiva 2002/58/CE

II. Obligación de poner los datos a disposición de los organismos del sector público y las instituciones, agencias u organismos de la Unión en caso de "necesidad excepcional".

El artículo 14.1 de la propuesta de Ley de Datos establece la obligación de los titulares de los datos de ponerlos a disposición de las autoridades públicas, instituciones, agencias y organismos de la UE en caso de "*necesidad excepcional*". El CCBE señala que este acceso se enmarca en los artículos 15, 16, 17 y siguientes. El alcance de la necesidad excepcional se define en el artículo 15 como la necesidad de responder a una emergencia pública, y el artículo 16 excluye las actividades realizadas para la prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas o la ejecución de sanciones penales, o para la administración aduanera o fiscal. El artículo 17 contiene las condiciones que deben cumplir las solicitudes.

Sin embargo, el CCBE expresa su profunda preocupación por este tipo de solicitudes de datos por parte de organismos públicos. Como subrayan la Junta Europea de Protección de Datos ("JEPD") y el Supervisor Europeo de Protección de Datos ("SEPD") "***los principios de necesidad y proporcionalidad, la base jurídica también debe definir el alcance y la forma del ejercicio de sus poderes por parte de las autoridades competentes e ir acompañada de garantías suficientes para proteger a las personas contra injerencias arbitrarias***"; a este respecto, la JEPD y el SEPD "***observan que las circunstancias que justifican el acceso no se especifican con precisión y consideran necesario que el legislador defina de forma mucho más estricta las hipótesis de urgencia o necesidad excepcional***"[6].

El CCBE considera que las amplias disposiciones sobre las solicitudes de datos de organismos públicos crean un riesgo de uso indebido, a pesar de que las condiciones de la propuesta establecen que (a) esta obligación de poner los datos a disposición de los organismos públicos no afectará a los datos personales y (b) que dichos datos no podrán utilizarse para la prevención, investigación, detección o enjuiciamiento de infracciones penales o administrativas, ejecución de sanciones penales, administración aduanera/tributaria, etc. La historia ha demostrado una y otra vez que es muy difícil hacer cumplir estas prohibiciones, y la diferencia entre datos no personales y datos personales es muy vaga incluso después de años de experiencias comunes con el RGPD, y cuantos más datos no personales a los que uno pueda tener acceso, más fácil es identificar o reducir de otro modo el posible ámbito de personas afectadas. Sin duda, habrá organismos públicos que cedan a la tentación de acceder fácilmente a tan vastas minas de datos, la cuestión es más bien cómo podremos averiguarlo.

Por ello, el CCBE considera que debe aclararse el ámbito de aplicación y las condiciones para poner los datos a disposición de los organismos públicos.

En cuanto a las justificaciones de una solicitud de datos por parte de organismos públicos, la propuesta exige la demostración de una "necesidad excepcional". Según el artículo 15, dicha "necesidad excepcional" se refiere a la necesidad de responder a una emergencia pública, prevenir o recuperarse de una emergencia pública, o cumplir una tarea de interés público previstas por la ley.

[6] Dictamen conjunto de la SEPD y el SEPD 02/2022 sobre la propuesta del Parlamento Europeo y del Consejo relativa a normas armonizadas sobre el acceso equitativo a la utilización de datos (Ley de datos), 4 de mayo de 2022, p. 3.

La noción de "emergencia pública" se define ampliamente en el apartado 10 del artículo 2 como "*una situación excepcional que afecte negativamente a la población de la Unión, de un Estado miembro o de una parte del mismo, con riesgo de repercusiones graves y duraderas en las condiciones de vida o en la estabilidad económica, o una degradación sustancial de los activos económicos de la Unión o del Estado o Estados miembros de que se trate*". Cabe señalar que el considerando (57) da ejemplos de emergencias públicas, como las emergencias de salud pública, las derivadas de la degradación del medio ambiente, las grandes catástrofes naturales o las provocadas por el hombre. El considerando se refiere *in fine* a las emergencias públicas determinadas según los procedimientos respectivos de los Estadosmiembros o de las organizaciones internacionales.

El CCBE considera que la falta de una definición clara de los conceptos de "necesidad excepcional", "emergencia pública", y la referencia a los procedimientos nacionales crea un alto riesgo de interpretaciones divergentes de los conceptos implicados y aumenta la probabilidad de interferencia con los derechos fundamentales. Apoya las recomendaciones del SEPD y del SEPB de modificar la propuesta para delimitar más claramente los tipos de situaciones que constituirían una emergencia.[7]

Además, el CCBE tiene preocupaciones similares sobre la justificación de una solicitud de datos cuando la falta de datos disponibles impide a la autoridad pública cumplir una tarea específica de interés público explícitamente prevista por la ley. Para esta justificación, el artículo 15(c) se refiere a dos situaciones: (1) cuando la autoridad pública no haya podido obtener datos por medios alternativos, incluso cuando no puedan aprobarse medidas legislativas a tiempo para que los datos estén disponibles, o (2) cuando la obtención de datos reduzca sustancialmente la carga administrativa.

A este respecto, el CCBE apoya las conclusiones de las autoridades europeas de protección de datos[8]y considera que:

- La posibilidad de solicitar datos, cuando las medidas legislativas no pueden adoptarse a tiempo, va en contra de las condiciones del apartado 1 del artículo 52 de la Carta de los Derechos Fundamentales de la UE, según el cual toda limitación de los derechos fundamentales debe estar prevista por la ley.
- La reducción de la carga administrativa no puede constituir una justificación suficiente para interferir en los derechos fundamentales.

Esta circunstancia debería retirarse de la propuesta, que debería definir mejor la justificación de una solicitud de datos.

Por último, mientras que los artículos 17(2)(c), 18(5) y 19(2) contienen disposiciones para proteger los secretos comerciales, **la propuesta no ofrece ninguna protección de los datos sujetos a PS/LPP.**

Como ya se ha dicho, la propuesta debe excluir la posibilidad de que los organismos públicos soliciten datos amparados por el secreto profesional, así como la obligación de que los titulares de los datos los revelen.

[7] EDPB-EDPS Dictamen conjunto 02/2022, §78

[8] Dictamen conjunto de la SEPD y el SEPD 02/2022, §79

III. Requisitos relativos al uso de servicios en nube

La Ley de Datos contiene disposiciones bastante detalladas relativas a los proveedores de servicios de tratamiento de datos, más comúnmente llamados proveedores de servicios en la nube, con el objetivo de ayudar a los usuarios de la nube a cambiar de proveedor de servicios (artículos 23 a 26, y 29). Además, los proveedores de servicios en la nube que no sean PYME tienen que "*adoptar medidas técnicas, jurídicas y organizativas razonables*" para impedir la transferencia internacional o el acceso gubernamental a datos no personales (artículo 27.1).

El CCBE señala que, en los últimos años, los servicios de computación en nube han madurado significativamente. Los procesos de seguridad se han hecho más sólidos, con certificaciones y garantías de terceros ampliamente aceptadas sobre la fiabilidad de los controles de seguridad informática. Sin embargo, siguen faltando algunos controles de seguridad de la información.

Mientras el servicio (o cualquier proveedor de plataforma o infraestructura subyacente) sea técnicamente capaz de leer y acceder a los datos del abogado, los riesgos de acceso no autorizado y, por tanto, de incumplimiento de las obligaciones de confidencialidad y de PS/LPP seguirán siendo una grave preocupación para los abogados. La reutilización de los datos de los clientes para otros fines o la interceptación ilegal de las comunicaciones por parte de las autoridades suscitan preocupaciones similares[9]

El CCBE trabaja actualmente en el uso de servicios en la nube por parte de los abogados en Europa.
El objetivo general de esta acción es adaptar el secreto profesional a la era digital definiendo mecanismos de defensa contra el acceso no autorizado a información amparada por el secreto profesional.

En este sentido, el CCBE pide a las instituciones de la UE y a los proveedores de servicios en la nube que tomen medidas para garantizar que se aplican medidas técnicas, jurídicas y organizativas razonables para evitar el acceso no autorizado a los datos cubiertos por PS/LPP.

IV. Requisitos esenciales de los contratos inteligentes

El artículo 30 establece que los vendedores de una aplicación que utilice contratos inteligentes deberán cumplir los requisitos esenciales enumerados, como la solidez, la terminación segura, etc., que servirán de base para una declaración de conformidad y cuyos detalles se establecerán posteriormente mediante normas.

Por lo que se refiere al artículo 30, el CCBE desea subrayar que en su forma actual, sin medidas provisionales, se trata de un planteamiento peligroso e innecesariamente precipitado. El CCBE cree firmemente que, independientemente de los medios técnicos que se utilicen, todas las partes deben mantener la protección de los consumidores y cualquier otra obligación jurídica establecida por ley.

La declaración de conformidad es una herramienta adecuada para los mercados maduros con normas vigentes sobre, por ejemplo, requisitos de seguridad o de otro tipo, ya que libera al regulador, entre otras cosas, de la carga de tener que actualizar con frecuencia los requisitos legislativos. Pero nunca se pretendió que sirviera para externalizar la carga reguladora a los grandes operadores del mercado que disponen de los recursos necesarios para enviar expertos a los organismos de normalización de la UE, como el ETSI.

[9] Guía sobre el uso de herramientas basadas en IA por abogados y bufetes de abogados en la UE, 2022, p. 47,48 y 51.

Nadie espera realmente ninguna orientación o norma en los próximos años sobre cómo los requisitos esenciales establecidos en la propuesta de Ley de Datos podrían aplicarse en los libros mayores distribuidos. No hay medidas transitorias o de aplicación que hagan referencia a los contratos inteligentes en la propuesta de Ley de Datos, y las cuestiones relativas a los contratos inteligentes no se investigaron en la evaluación de impacto. Se trata más de un problema de seguridad jurídica y de idoneidad del enfoque normativo previsto que de un problema directo de los abogados, pero las empresas europeas probablemente acudirán a sus abogados en la UE en busca de orientación en estas cuestiones y, sobre la base de las disposiciones actuales, los abogados no podrán proporcionar dicha orientación.

Por lo tanto, el CCBE considera que las amplias obligaciones del artículo 30 no están suficientemente justificadas y no respetan el principio de neutralidad tecnológica. Estas disposiciones deberían eliminarse de la propuesta.