



Representando a los  
Abogados europeos

---

**COMENTARIOS DE CCBE SOBRE EL CONTROL  
DE LOS MEDIOS ELECTRÓNICOS POR PARTE  
DE LOS ESTADOS (INCLUIDOS LOS DATOS DE  
ABOGADOS EUROPEOS)**

**Consejo de la Abogacía Europea**

*association internationale sans but lucratif*

Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail  
ccbe@ccbe.org – www.ccbe.org

---

---

## Comentarios de CCBE sobre el control de los medios electrónicos por parte de los Estados (incluyendo los datos de abogados europeos)

---

### Antecedentes

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 32 países miembro y a 11 países asociados y observadores, así como a cerca de un millón de abogados europeos.

El 1 de julio de 2013, CCBE publicó una declaración (véase en el anexo de la presente declaración) sobre prácticas gubernamentales que implican el control y análisis de datos, sobre todo su contenido, en la que CCBE expresaba su profunda preocupación respecto a que uno de los valores principales de la profesión, como es el secreto profesional, conocido en algunos países como el privilegio legal de la profesión, se encuentre en una situación de grave riesgo, ya que la merma de este aspecto de la confidencialidad, desgasta también la confianza de los ciudadanos en el Estado de Derecho.

La declaración de CCBE estaba basada en informes sobre violaciones masivas, generalizadas, del derecho fundamental a tener una vida privada y personal, que están siendo llevadas a cabo de forma sistemática por las agencias gubernamentales de las principales potencias occidentales, incluidos los Estados miembro de la UE. Tales afirmaciones indican una clara vulneración de la Carta de Derechos Fundamentales de la UE por parte de determinados gobiernos de países miembro de la UE, principalmente suponen la vulneración de los artículos 7<sup>1</sup> y 8<sup>2</sup>, y también, debido a la falta de algún mecanismo apropiado de revisión judicial (art. 47<sup>3</sup>).

En relación al supuesto acceso indiscriminado y al control masivo de la mayoría de las comunicaciones entre ciudadanos no estadounidenses, señalar que también supone el acceso a las comunicaciones existentes entre los abogados y sus clientes. Somos de la opinión de que este tipo de control o vigilancia va más allá de poner en riesgo determinados derechos humanos entre particulares, pues supone una amenaza contra el Estado de Derecho, reconocido en las actuales democracias.

A día de hoy, no se han publicado por la Unión Europea ni por sus Estados miembro, Informes que aborden satisfactoriamente las denuncias antes mencionadas. Sin ninguna base sólida para los hechos en este tema, no hay forma de saber si existe vulneración de los derechos fundamentales, como el artículo 8, párrafo 2m de la Carta Fundamental de Derechos Humanos de la Unión Europea, o el art. 12 de la Directiva de Protección de Datos (95/46/EC), que

---

<sup>1</sup> **Artículo 7 – Respeto de la vida privada y familiar**

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

<sup>2</sup> **Artículo 8 – Protección de datos de carácter personal**

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

<sup>3</sup> **Artículo 43 – El Defensor del Pueblo**

Todo ciudadano de la Unión Europea o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a someter al Defensor del Pueblo de la Unión los casos de mala administración en la acción de las instituciones u órganos comunitarios, con exclusión del Tribunal de Justicia y del Tribunal de Primera Instancia en el ejercicio de sus funciones jurisdiccionales.

también hace imposible cualquier intento de hacer valer estos derechos. Cada ciudadano de la UE tiene derecho a acceder a sus datos personales y ello incluye también el derecho a saber si ha sufrido alguna intrusión ilícita en su vida cibernética privada por parte de un Estado. También constituye un problema que las negociaciones bilaterales con Estados Unidos no hayan sido del todo transparentes hasta la fecha.

En base a otros informes de prensa y a las recientes audiencias del Comité de Libertades Civiles del Parlamento Europeo, CCBE considera que las mayores amenazas a la confianza de los clientes en el ámbito del secreto profesional tienen dos causas: a) la falta de confianza en los organismos estatales que gozan del privilegio de investigación secreta (existe la preocupación de que estas facultades van a ser utilizadas fuera de los límites de la democracia) y, b) una carencia objetiva de medios técnicos a disposición de los despachos de abogados para asegurar un ejercicio efectivo del secreto profesional.

En todos los Estados miembro de la UE, el secreto profesional de los abogados está fuertemente protegido, aunque los límites y los medios de protección legal sean diferentes. Tanto la jurisprudencia del Tribunal de Justicia de la Unión Europea como del Tribunal Europeo de Derechos Humanos reconocen este derecho. Sin embargo, con base a ello, recientemente se ha revelado información sobre la práctica de los principales organismos de control del Estado, habiéndose originado la preocupación de que la protección ofrecida por los medios jurídicos de los Estados miembro de la UE para el secreto profesional no funciona en la práctica.

### **No hay confianza sin confidencialidad - repercusiones en la Agenda Digital para Europa**

El rol principal del abogado, ya sea contratado por una persona física, por una sociedad o por el Estado, es la confianza del cliente en éste como un profesional respetado y participante indispensable en la buena administración de la justicia y la democracia. La esencia de la función del abogado es que éste escucha todas aquellas cuestiones que su cliente no le va a contar a ninguna otra persona - los detalles personales más íntimos o los secretos más valiosos a nivel comercial - en los que el abogado es destinatario de esta información basada en la confianza. Sin la garantía de confidencialidad, no puede haber confianza. Por lo tanto, si el derecho de los ciudadanos de la UE y de las empresas a ser protegidos contra cualquier divulgación de las comunicaciones habidas con su abogado es negado, se le estaría denegando el acceso a la asistencia letrada y a la justicia.

Estudiando la situación de los instrumentos técnicos existentes a disposición de los despachos de abogados, incluyendo las grandes firmas, CCBE se ha percatado que los abogados están utilizando en la actualidad sistemas de comunicaciones electrónicas y para los servicios en la nube, y que no son seguros porque ahora sabemos que fueron diseñados con ciertas irregularidades para que las agencias gubernamentales pueden acceder a ellos. Sin embargo, como hemos conocido recientemente, hasta las más grandes de estas agencias gubernamentales tienen problemas en ocasiones para controlar la información secreta a la que tienen acceso. Es evidente que cuantas más “puertas traseras” haya, menos segura será la infraestructura online.

Si los abogados están usando este tipo de comunicaciones electrónicas inseguras o servicios en la nube, ellos mismos están de hecho infringiendo sus obligaciones como responsables del tratamiento de datos personales de sus clientes e incumpliendo las normas deontológicas. Este problema de tener que utilizar comunicaciones inseguras no es simplemente un problema de

formación o cultural, sino más bien un problema de todas las empresas europeas, a excepción de las más grandes o de aquellas que trabajan en defensa de la industria.

Como consecuencia de ello, los abogados se ven abocados a situaciones en las que tienen que elegir entre alguna de las siguientes opciones:

- a) continuar utilizando las comunicaciones electrónicas y los servicios de la nube que el público en general utiliza, sabiendo que están quebrantando sus obligaciones con los clientes de mantener la confidencialidad de la información, y simplemente pedir a los clientes su consentimiento informado acerca de tales riesgos; o
- b) utilizar servicios de comunicaciones electrónicas que hayan sido creados por nuevas inversiones en la construcción de una única Unión Europea, de forma totalmente independiente con políticas de privacidad estrictas y que se logre, por tanto, la reconstrucción de la confianza a nivel europeo - a la vez que la aceptación de la ineficacia de tales soluciones, como por ejemplo, los costes de reconstrucción; o
- c) no usar el email, servicios de comunicación electrónica o los servicios de la nube en las comunicaciones con clientes, el intercambio de datos sólo debe usarse a modo de soporte de datos físicos, como flash drives o confiar en las máquinas de escribir y los servicios postales y de correo rápido.

Debe quedar claro que ninguna de las alternativas anteriores es realista en la práctica y que esta situación es completamente inaceptable en una sociedad democrática basada en el Estado de Derecho.

Esto, a su vez, también tendrá repercusión para el futuro de la Agenda Digital para Europa, cuyo principal objetivo es ayudar a los ciudadanos y a las empresas europeas para sacar el máximo partido a las tecnologías digitales. Sin embargo, como se indica en la Agenda Digital para Europa, "los europeos no abrazarán las tecnologías si no confían en ellas- la era digital no es ni el "gran hermano" ni el "salvaje oeste cibernético"<sup>4</sup>". Como se expone más arriba, ello supone un hecho significativo en el caso de los abogados. Mientras el secreto profesional entre abogado y cliente no pueda ser garantizado, la prestación efectiva de los servicios jurídicos estará seriamente debilitada. Dada la importancia de la relación entre los servicios jurídicos y el rendimiento económico - derivada de las funciones que desempeñan los servicios jurídicos para facilitar y sostener los mercados - esta situación tendrá un impacto negativo sobre la economía europea.<sup>5</sup>

### **Reconstruir la confianza**

Basada en la información recientemente revelada en relación a la práctica de determinadas agencias de control estatal, se ha puesto de manifiesto la preocupación de que la protección ofrecida por los mecanismos legalmente previstos por los Estados miembro de la UE para el secreto profesional, podrían no haber funcionado en la práctica, y podría haber habido casos en los que los Estados miembro de la UE hayan permitido un control electrónico contra sus propios ciudadanos, vulnerando sus propias legislaciones.

---

<sup>4</sup> Comunicación de la Comisión, Una Agenda Digital para Europa, página 16 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>

<sup>5</sup> Ver Oposición a las Políticas de Regulación, del profesor George Yarrow y el Dr. Christopher Decker, [http://www.cbbe.eu/fileadmin/user\\_upload/NTCdocument/RPI\\_study\\_Yarrow\\_D1\\_1348650358.pdf](http://www.cbbe.eu/fileadmin/user_upload/NTCdocument/RPI_study_Yarrow_D1_1348650358.pdf), agosto de 2012. En la página 3 se señala que "Una relación particularmente importante entre los servicios jurídicos y los resultados económicos se debe a los roles que desempeñan los servicios jurídicos para ayudar y sostener al mercado. La actividad principal del sector profesional de servicios jurídicos tiende a ampliar la actividad en el mercado a través de la economía, y que está estrechamente vinculada a la productividad y el crecimiento económico.

Además, si en un Estado miembro de la UE, un abogado solicita una orden judicial para acceder a información confidencial habida o mantenida por abogados en otro país, la solicitud no puede ser atendida si el órgano jurisdiccional emisor está establecido en un país extranjero, sin posibilidad alguna de ser supervisado por un juez en el país donde el abogado reside. Del mismo modo, razones de seguridad del otro Estado, perteneciente o no a la UE, no lo justifican como motivos de seguridad nacional en el propio Estado miembro, y por ello las agencias de seguridad nacional de un Estado miembro de la UE no deberían cooperar en este tipo de vigilancia sin respetar las normas nacionales sobre el secreto profesional.

Reconociendo la necesidad de que los organismos gubernamentales, en aplicación de la ley y de la seguridad nacional, lleven a cabo un control electrónico a los ciudadanos en determinadas circunstancias, la pérdida de confianza que se ha generado sólo puede ser ahora tratada por la vía política: por ejemplo, analizando de forma cautelosa qué áreas de la vigilancia secreta no deben publicarse y, como controlarlo, dónde podría resultar útil la participación civil (incluso a través de los representantes de la profesión legal) para recuperar y mantener la confianza de los ciudadanos.

### **Recomendaciones**

1. En relación al [posicionamiento](#) de CCBE (adoptado el 7/09/2012) sobre la protección de datos propuesto en el paquete de reformas; CCBE considera que las obligaciones de las autoridades policiales y judiciales en relación con la protección de los datos personales y otros datos sujetos al secreto profesional, debería ser al menos tan elevada como la protección esperada por los datos de control de los organismos operantes en el sector privado. Esto refuerza la necesidad de contar con un régimen de protección de datos único y completo.
2. Además, se deben tomar medidas a nivel de la UE, al objeto de establecer un nivel mínimo de protección legal permitido para el secreto profesional, dada la vigilancia electrónica de los gobiernos, incluido el uso de los servicios de comunicación electrónica o de otros servicios en la nube para las comunicaciones entre abogado y cliente. El uso de estas facilidades entre el abogado y el cliente debería ser protegido de la misma forma y con independencia de si están almacenados en un centro de datos o en un ordenador en el despacho de un abogado o en un ordenador particular del abogado. El contenido que contiene el secreto profesional y que es procesado por un servicio de comunicación electrónica o por un proveedor de la nube (incluyendo el proveedor del email), no debería ser accesible para las agencias gubernamentales. Los servicios de comunicación electrónica y la nube deberían estar obligados a ofrecer a los abogados una opción para indicar la información-por supuesto, sólo después de una cuidadosa verificación para comprobar si el usuario es realmente un abogado.
3. Deberían establecerse normas mínimas a nivel europeo en materia de vigilancia electrónica, en concreto fijando límites razonables al hecho de poder invocar la seguridad nacional como motivo para restringir el derecho a la intimidad. Dicho trabajo de reglamentación debe basarse en los informes y sugerencias que ya se han realizado a nivel regional e internacional en esta materia, como por ejemplo el informe de Frank La Rue, reportero especial del Consejo de Derechos Humanos de las Naciones Unidas (ver este [enlace](#)) o el borrador del Comité de la Asamblea Parlamentaria del Consejo Europeo, "Compilación de buenas prácticas y medidas legales que garanticen por parte de las agencias de inteligencia; el respeto a los derechos humanos, en la lucha contra el terrorismo, en concreto, en su supervisión" (ver este [enlace](#)).

4. La UE debería trabajar hacia el reforzamiento de la privacidad a nivel internacional, por ejemplo sobre la base de protocolos facultativos del artículo 17 del Convenio Internacional de Derechos Civiles y Políticos, y reforzando el nivel de protección garantizado en la práctica por los principios fundamentales. En cuanto a los países europeos que se encuentran fuera del Espacio Económico Europeo, en el marco del proceso de modernización de la convención, la UE debe apoyar la adopción de excepciones al amparo del art. 9 de la Convención para la Protección de Datos de Carácter Personal.
  
5. Más allá de todas las medidas de protección necesarias que pueden ser alcanzadas mediante políticas y normativas, las medidas técnicas tienen que ser tomadas también para reconstruir la confianza en las comunicaciones electrónicas y en los servicios de la nube. Además de las medidas técnicas destinadas a hacer Internet y los servicios de la nube más seguros y a controlar el acceso por parte de los gobiernos, también hay que tener en cuenta los requisitos específicos que deben cumplirse en relación con la información que esté sujeta al secreto profesional, como la que existe entre un abogado y su cliente. En otras palabras, las comunicaciones electrónicas y las infraestructuras de los servicios de la nube deben ser configurados de forma que las funcionalidades técnicas garanticen que los gobiernos o terceros no hagan un abuso del acceso a las mismas.

### **Conclusión**

CCBE, además, urge a las instituciones de la UE a crear el marco legal y tecnológico necesario con el objeto de mejorar la actual situación que afecta al control electrónico de los ciudadanos y a salvaguardar el secreto profesional, que es un derecho de todos los ciudadanos de la UE y uno de los principales valores de la abogacía.

ANEXO: Posicionamiento del CCBE sobre las prácticas gubernamentales de control sobre las actividades de búsqueda y procesamiento de datos en masa