Consejo de la Abogacía Europea
Asociación internacional sin ánimo de lucro
Rue Joseph II, 40 /8 – 1000 Bruselas
T. : +32 (0)2 234 65 10 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

Recomendaciones de CCBE para la protección del secreto profesional en el contexto de las actividades de vigilancia

28/04/2016

RESUMEN EJECUTIVO

"*El deber de confidencialidad del abogado sirve al interés de la administración de justicia, así como al interés del cliente. Por consiguiente merece una protección especial por el Estado.*"

– artículo 2.3 del Código Deontológico de CCBE

El objetivo del presente documento es informar a los legisladores y políticos europeos acerca de los valores que deben preservarse para garantizar que los principios esenciales del secreto profesional y la confidencialidad no sean menoscabados por las actuaciones del estado, interceptando las comunicaciones y accediendo a la información de los abogados con fines de vigilancia o de ejecución.

La primera parte de las recomendaciones propuestas aborda el significado y alcance del principio de confidencialidad de las comunicaciones abogado-cliente consagrado por la normativa europea y el CEDH, así como numerosa jurisprudencia. El documento expone que la confidencialidad de las comunicaciones abogado-cliente, están protegidas en virtud de las normas UE y del CEDH y reviste una importancia particular a la vista de los tribunales europeos y otros organismos implicados. La confidencialidad no es solo un deber del abogado, sino también un derecho fundamental del cliente. Sin la certidumbre de la confidencialidad, no puede existir confianza, que es justamente el elemento clave del buen funcionamiento de la administración de Justicia y del Estado de Derecho.

Las recomendaciones de la segunda parte buscan garantizar el respeto de este principio enunciando las siguientes condiciones principales:

1. Principio fundamental: cualquier actividad de vigilancia, directa o indirecta, por parte del Estado debe inscribirse dentro de los límites del Estado de Derecho y debe respetar el principio según el cual las comunicaciones realizadas dentro del secreto profesional son inviolables y no pueden estar sometidas a interceptaciones o vigilancia.

2. Necesidad de control legislativo: todas las actividades de vigilancia deben estar reguladas con un grado de precisión suficiente en la legislación primaria, previendo una protección explícita de las comunicaciones abogado-cliente. En el caso de que las actividades de vigilancia fueran confiadas a empresas privadas, el gobierno debe detentar, siempre, el control completo del conjunto de los procesos de vigilancia. La desencriptación de los datos protegidos no puede autorizarse más que por vía judicial, a través de un proceso y una autorización por parte de un juez.

3. Campo de aplicación de las excepciones autorizadas: sólo se podrán interceptar las comunicaciones que estén fuera del ámbito del secreto profesional. Ningún sistema actual las protege si el abogado está implicado en la persecución de delitos penales, siendo el objetivo asegurar la inviolabilidad del secreto profesional. Así, toda orden de interceptación de comunicaciones a un abogado no puede acordarse a menos que existan pruebas convincentes de que se vaya a proteger el secreto profesional.

4. Control judicial independiente: es indispensable que exista una autorización judicial antes de toda interceptación de comunicaciones a abogados. Así, un órgano judicial independiente podrá poner fin a la interceptación y también destruir la información recogida – debe controlar todo el proceso de vigilancia. La ley debe establecer la asignación de poder al juez, para que tome medidas de ejecución.

5. Uso de la información interceptada: si lo ha sido sin autorización judicial previa, y por tanto atenta contra el principio del secreto profesional, debe declararse inadmisible ante un tribunal y ser destruida. Si ha sido obtenida de manera legal, podrá ser utilizada como prueba.

6. Vías de recurso y sanción: indispensables para abogados y clientes víctimas de vigilancia ilegal, así como la instauración de un sistema de sanciones. Los abogados y sus clientes tienen derecho a ser informados respecto a las informaciones recabadas en actividades de vigilancia respecto a los datos de actividades de vigilancia directa o indirecta, una vez que se sepa que ésta se ha realizado.

ÍNDICE

INTRODUCCIÓN

En los últimos años CCBE ha expresado su preocupación respecto a las revelaciones de los métodos de trabajo de los servicios de inteligencia nacionales. Estas preocupaciones se refieren en particular a organismos estatales teniendo competencias de investigación secreta y/o insuficientemente controlada, así como la utilización de tecnologías de intercepción y seguimiento extremadamente sofisticadas y de gran alcanza para acceder a las comunicaciones que pertenece a los ciudadanos de manera indiscriminada, a gran escala y sin levantar sospecha. A pesar de que estas tecnologías pudiesen llevar consigo beneficios en la lucha contra el terrorismo el crimen organizado, también surgen numerosos problemas específicos que tiene que ser abordados, especialmente aquellos referentes a la legalidad en la interferencia en los Derechos Fundamentales.

Esta interferencia se vuelve particularmente peligrosa cuando los datos y comunicaciones a los que los gobiernos han accedido son aquellos a los que las leyes les han amparado con una protección especial. Este es el caso ciertamente en relación con las comunicaciones entre los abogados y sus clientes. En todos los Estados miembros, la ley protege la divulgación de información comunicada en confidencia entre el abogado y su cliente. Sin esta protección, el mismo Estado de derecho se ve socavado.

En especial, el acceso a la justicia, el derecho a un juicio justo y el secreto profesional se pueden ver vulnerados. Estos derechos se protegen en numerosos instrumentos nacionales e internacionales, incluidos el Convenio Europeo de Derechos Humanos (CEDH) y la Carta de los Derechos Fundamentales de la UE. La vulneración del secreto profesional significa una violación de las obligaciones internacionales, denegar los derechos del acusado, y en general poner en compromiso la naturaliza democrática del Estado.

Esto ha sido reconocido por varios organismos internacionales. Por ejemplo, el Parlamento Europeo en octubre de 2015 adoptó una resolución de seguimiento sobre vigilancia masiva electrónica de ciudadanos de la UE que subraya que los derechos de los ciudadanos deben ser protegidos contra cualquier vigilancia de las comunicaciones entre los abogados. Más aún, el Parlamento Europeo hizo pidió a la Comisión Europea que adoptase una comunicación en este sentido. Asimismo, el Consejo de Europa adoptó y publicó varios informes sobre este asunto en 2015. La Asamblea Parlamentaria adoptó una resolución destacando que la intercepción de comunicaciones privilegiadas de los abogados pone en peligro los Derechos fundamentales, y en particular el derecho a la protección del secreto profesional y el derecho a un juicio justo. La Comisión de Venecia ha publicado una actualización de un informe previo sobre el control democrático los servicios de seguridad y de inteligencia, que reconoce que se debe otorgar una alta protección a las comunicaciones abogado-cliente, incluyendo las garantías procesales y una supervisión exterior fuerte. Por último, el Comisario para los Derechos Humanos subrayó en un documento de trabajo que la intercepción de comunicaciones entre el abogado y su cliente puede perjudicar la igualdad de medios y el derecho a un juicio justo.

Por tanto, no se puede sobrestimar la importancia de este principio, y se encuentra aún hoy en día gravemente amenazado. Los últimos avances llevados a cabo en varios países europeos comprometen la protección tradicionalmente proporcionada al secreto profesional y a la confidencialidad en los países democráticos.

El objetivo del presente documento es informar a los legisladores y políticos europeos acerca de los valores que deben preservarse para garantizar que los principios esenciales del secreto profesional y la confidencialidad no sean menoscabados por las actuaciones del estado, interceptando las comunicaciones y accediendo a la información de los abogados con fines de vigilancia o de ejecución.

El documento no busca establecer un enfoque europeo común como tal, ya que se reconoce que existen importantes diferencia entre el secreto profesional y la confidencialidad, y que podría haber diferencias entorno a la comprensión de la concreta naturaleza y alcance del secreto profesional entre las diferentes jurisdicciones. No obstante, sea cual sea el concreto enfoque que se aplique en

cada jurisdicción, todos los Estados miembros del Consejo de Europa se encuentran vinculados por el Convenio Europeo de Derechos Humanos (CEDH) y, además, los Estados miembros de la UE están también vinculados por el derecho de la UE. Por tanto, el enfoque del presente documento está dirigido a llevar a cabo un análisis del enfoque adoptado por el Tribunal Europeo de Derechos Humanos (TEDH) y el Tribunal de Justicia de la Unión Europea (TJUE), para identificar los principios mínimos que se aplican en toda Europa. Por supuesto, se da por hecho que algunas jurisdicciones estarán aplicando unos principios que excedan de estos mínimos que analizaremos.

A efectos de este documento, a los conceptos de "estado" y "gobierno" se les otorga deliberadamente un significado amplio e impreciso, ya que estos términos podrían referirse al gobierno nacional, al gobierno en diferentes niveles (federal, regional o local), a las agencias gubernamentales, a las autoridades fiscales, a las agencias independientes que lleven a cabo funciones de derecho público, a la policía, a la fiscalía, a los servicios de inteligencia y a otros. Las presentes recomendaciones hacen referencia al acceso por parte del estado a la información y a las comunicaciones entre los clientes y los abogados, en todas sus formas y manifestaciones.

PARTE I: SECRETO PROFESIONAL Y CONFIDENCIALIDAD – SIGNIFICADO Y ALCANCE

El texto íntegro del cuerpo del documento pueden encontrarlo en inglés en el siguiente enlace.

PARTE II: RECOMENDACIONES DE CCBE

El análisis jurídico precedente afirma la posición de CCBE de la cual las comunicaciones y los datos protegidos por el secreto profesional y las obligaciones del secreto profesional son inviolables y no se puede someter a intercepciones ni vigilancia. Las siguientes recomendaciones buscan asegurar el respeto de este principio.

1. Principio General

Cualquier vigilancia directa o indirecta llevada a cabo por el Estado debería estar sujeta a las reglas del estado de Derecho y, en particular, esa vigilancia debería respetar la protección otorgada al secreto profesional. La protección es, en asuntos contenciosos, un componente esencial para garantizar el derecho a un juicio justo y en todos los casos es un principio fundamental para el estado de derecho.

2. Necesidad de un control legislativo

2.1 Todas las actividades de vigilancia necesitan ser reguladas con una especificidad adecuada (por ejemplo, una definición clara de "seguridad nacional") y transparencia.

No puede darse el caso que en una sociedad democrática, se permita a los servicios de seguridad a no ser transparentes, irresponsables y operen fuera del marco jurídico vinculante. Sin esos controles, hay un riesgo de incumplimiento arbitrario de los Derechos Humanos en general y el secreto profesional en particular. Introducir el mandato de las agencias de inteligencia en la legislación primaria es un requisito del CEDH.[1]

En algunos Estados donde hay un marco regulatorio, se han incorporado importantes protecciones no en la legislación primaria sino en códigos de práctica no vinculantes, líneas directrices (y por ejemplo, en el caso de Reino Unido bajo la "Regulation of Investigatory Powers Act 2000", importantes áreas de la regulación y el control no se encuentran en la ley sino en códigos de práctica no vinculantes). Aunque semejantes códigos y guías puedan tener su lugar, una protección substantiva del secreto profesional debe consagrarse en la legislación primaria, para que los servicios de inteligencia rindan cuenta ante los tribunales por como desempeñan sus funciones.

2.2 La legislación sobre las actividades de vigilancia necesita probar protección explícita del secreto profesional y remover los ataques deliberados a las comunicaciones entre el cliente y el abogado del ámbito de las atribuciones del poder de las agencias de inteligencia.

El nivel de protección del secreto profesional debe siempre estar al nivel más alto, independientemente de si las medidas de vigilancia se toman por motivos policiales (por ejemplo por la policía o los servicios judiciales) o para la protección de la seguridad nacional (por ejemplo por agencias de inteligencia nacionales). La naturaleza intrusiva y el impacto potencial en ambos tipos de

[1] Council of Europe Venice Commission, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e 2015, page 18: "Most democratic states, in recognition of the impact strategic surveillance has on human rights, have placed at least part of the mandate of the signals intelligence function in primary legislation. [This] is also a requirement of the ECHR."

actividades sobre el derecho individual a un juicio justo son idénticos y por lo tanto requiere un alto nivel de protección legal.

Una historia con moraleja en el Reino Unido es el caso *Re McE*[2]. En ese caso, la Casa de los Lores interpretó la falta de una protección específica del secreto profesional como la permisión implícita de interceptar material legalmente confidencial, resultando en que el Parlamento haya decidido invalidar el secreto profesional. La decisión ha sido ampliamente criticada pero se debe subrayar que el texto propuesto de la nueva legislación que fue debatido en el Parlamento reproduce la redacción del 2000 Acto con la intención de privar de protección al material cubierto por el secreto profesional.

2.3 La legislación debe proporcionar suficientes garantías en el caso de la externalización completa o parcial de actividades de vigilancia a entidades privadas, para asegurar que el gobierno siempre esté en control y sea completamente responsable de todo el proceso de vigilancia, los datos y el uso de los datos.

La externalización de actividades de vigilancia a entidades privadas puede desviar la responsabilidad de los servicios policiales, judiciales o de seguridad nacional a empresas más pequeñas que no pueden ser responsables ante prohibiciones constitucionales. Por lo tanto, las entidades privadas que están involucradas en el proceso de vigilancia deben estar sujetas a rigurosas normas deontológicas y requisitos de confidencialidad y estar bajo obligaciones contractuales de dar transparencia y acceso gubernamental a sus disposiciones técnicas y organizativas que rigen sus actividades de vigilancia. Las entidades estatales deben ser asignadas con suficientes conocimientos técnicos y recursos para permanecer en control de cualquiera de las actividades de vigilancia que son externalizadas a las empresas privadas.

2.4 La legislación no debería impedir a los abogados de proteger adecuadamente la confidencialidad de las comunicaciones con sus clientes (por ejemplo a través de métodos de encriptación), y no deberían dar autorización a las fuerzas orden o judiciales acceso privilegiado a los datos encriptados.

Los abogados guardan información sensible (desde secreto comerciales a detalles de su vida privada) que fue proporcionada por sus clientes en confidencia y no podrá divulgarse. Esto vuelve a los abogados particularmente vulnerables ante ataques ilícitos por gobiernos o hackers privados y requiere una protección criptográfica adecuada. El derecho a la protección de datos también cubre la seguridad de datos, como recogen los artículos 8 del CEDH y 6 de la Carta de Derechos Fundamentales de la UE[3], así como el Convenio sobre protección de datos del Consejo de Europa de 1981 y la actual Decisión Marco sobre la protección de datos de 2008. Sin embargo, la falta de seguridad podría afectar a un grupo de derechos aún más amplio, como los derechos económicos, los de privacidad o los de un proceso justo[4]. Por tanto, la desencriptación solo puede permitirse si se encuentra legalmente definido y cualquier decisión que permita la desencriptación de las comunicaciones protegidas entre abogado y cliente debe ser adoptada por un juez independiente, caso por caso y seguida de un proceso justo.[5]

3. El alcance de la interceptación admisible

3.1 Solo pueden interceptarse las comunicaciones que queden fuera del alcance del secreto profesional o la confidencialidad.

[2] House of Lord, http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090311/mce-1.htm 2009, UKHL 15.
[3] Ibid.
[4] Ibid.
[5] Ibid.

Como se ha mencionado anteriormente,

El texto íntegro del cuerpo del documento pueden encontrarlo en inglés en el siguiente enlace.

CONCLUSIÓN

Dado que el garantizar la seguridad se considera una obligación del Estado hacia sus ciudadanos, el secreto profesional y la confidencialidad resultan elementos esenciales del estado de derecho. Cuando el Estado trate de limitar o menoscabar los principios de secreto profesional y confidencialidad, aunque sea en nombre de la seguridad nacional, ello constituye en sí un ataque al estado de derecho.

No obstante, el conflicto que supuestamente existe entre la necesidad de proteger la seguridad nacional por un lado, y la defensa del secreto profesional y la confidencialidad por otro, es ilusoria. Ambos pueden coexistir como componentes esenciales de una sociedad democrática madura y plenamente funcional, que se rija de acuerdo al estado de derecho. El objetivo del presente documento ha sido el exponer con claridad cómo se podría alcanzar dicho fin.

Antecedentes históricos – Las actuaciones de CCBE en relación a la vigilancia

Desde que salieran a la luz las revelaciones de Edward Snowden en 2013, CCBE ha publicado declaraciones, estudios y cartas para denunciar las vulneraciones del secreto profesional por parte de los estados y los cuerpos gubernamentales que llevan a cabo actividades de vigilancia ilegal.

A principios de julio de 2013, CCBE publicó su primera declaración de denuncia de la amenaza que representan los cuerpos del estado con poderes de investigación secreta y tecnologías de intercepción sofisticadas.

En octubre de 2013, CCBE trazó sus primeras recomendaciones para salvaguardar el secreto profesional frente a la vigilancia gubernamental.

En diciembre de 2013, CCBE participó en el Comité de Investigación de LIBE sobre la Vigilancia Electrónica en Masa de los ciudadanos de la UE. Tras una investigación de seis meses, el Parlamento Europeo aprobó en 2014 una resolución que concluía, entre otros asuntos, que es "*crucial que la confidencialidad profesional de los abogados (…) se encuentre salvaguardada frente a las actividades de vigilancia en masa*" y "*cualquier incertidumbre sobre la confidencialidad de las comunicaciones entre los abogados y sus clientes podría tener un impacto negativo en los derechos de los ciudadanos de la UE de acceso al asesoramiento jurídico y acceso a la justicia, así como el derecho a un juicio justo.*" Esta misma resolución también propone el establecimiento de un "*Habeas Corpus* digital" para proteger los derechos fundamentales, incluidos el estado de derecho y la confidencialidad de las comunicaciones abogado-cliente. Esta resolución fue acogida con satisfacción por parte de CCBE.

En abril de 2014, CCBE publicó un estudio comparativo sobre la vigilancia gubernamental de los datos almacenados por los abogados en la nube, señalando en qué medida dichos datos electrónicos son susceptibles de acceso gubernamental en las diferentes jurisdicciones europeas, y las normas y condiciones que rodean dicho acceso.

A raíz de los importantes avances en relación a las actividades de vigilancia gubernamental y su influencia sobre los abogados y sus clientes, en marzo de 2015 CCBE decidió establecer un grupo de trabajo específico sobre vigilancia.

En marzo de 2015, CCBE escribió al Ministro de Inmigración y Seguridad de Reino Unido y al Ministro de Estado de la Oficina de Exteriores y Commonwealth. Las cartas expresaban la preocupación por la existencia de políticas en Reino Unido que permitían el acceso por parte del personal de los servicios de seguridad a las comunicaciones confidenciales abogado-cliente, y buscaban aclaraciones sobre el asunto. Finalmente, CCBE escribió en enero de 2016 al Mariscal del Parlamento Polaco, expresando la preocupación por un proyecto de ley sobre modificaciones al estatuto de los policías y otras normas relacionadas con los servicios secretos del estado, y en particular, en relación al reglamento sobre vigilancia de datos y almacenamiento de datos.

Además, CCBE ha participado en dos casos ante los tribunales. En el primero, CCBE intervino en 2015 ante el Consejo Constitucional Francés para defender la confidencialidad de las comunicaciones entre los abogados y sus clientes. Presentó sus alegaciones como parte de la revisión de la norma sobre inteligencia y formuló varias propuestas para que la ley respetara el derecho a la privacidad y el derecho al asesoramiento jurídico. En el segundo, en mayo de 2015 CCBE intervino de manera exitosa ante el Juzgado de Primera Instancia de La Haya, en un asunto presentado contra el Estado Neerlandés por el despacho de abogados Prakken d'Oliveira y la Asociación Neerlandesa de Abogados Defensores Penales (NVSA). Se cuestioné al juzgado por la legalidad de las escuchas por parte de las agencias internas de inteligencia sobre las llamadas y las comunicaciones de los abogados. En su sentencia dictada el 1 de julio, el juzgado reconoció que la capacidad de comunicarse de manera confidencial con un abogado es un derecho fundamental que fue vulnerado de acuerdo a la política de vigilancia neerlandesa. Por ello, el juzgado ordenó al gobierno neerlandés detener todas las interceptaciones de las comunicaciones entre los clientes y sus abogados en un plazo de seis meses. Como respuesta, el Estado Neerlandés inmediatamente interpuso una apelación contra la sentencia. El 25 de agosto de 2015 CCBE se opuso a las alegaciones de la apelación, y el 27 de octubre de 2015 el Tribunal Neerlandés de Apelación desestimó íntegramente el recurso presentado por el Estado Neerlandés, confirmando la sentencia dictada por el Juzgado de Primera Instancia, por la que se prohibía la vigilancia de las comunicaciones protegidas por el secreto profesional.