La ciberseguridad en la abogacía: una aproximación deontológica
(Informe 12/2018)

1. LA ABOGACÍA Y LA CIBERSEGURIDAD

El Preámbulo de la Estrategia Nacional de Ciberseguridad de 2013[1] (ENCS) termina diciendo que nuestra dependencia del ciberespacio *nos obliga a dedicar todos los medios necesarios a la hora de poner nuestras capacidades al servicio de la ciberseguridad. El entorno es dinámico y son muchas las incertidumbres y retos que afrontamos. Únicamente si nos comprometemos de forma decidida con la seguridad del ciberespacio, la competitividad de nuestra economía y la prosperidad de España serán una realidad posible.*

La abogacía es un colectivo donde los riesgos cibernéticos a los que se enfrenta son especialmente relevantes, en particular a la vista de la cantidad pero, sobre todo, de la sensibilidad y relevancia de la información, propia y ajena, que manejan estos profesionales.

En el concreto caso de la abogacía española, basta con leer el preámbulo del proyecto de Estatuto General aprobado por el Pleno del Consejo General de la Abogacía Española en 2013, aún pendiente de aprobación por el Gobierno, para recordar que esta es una profesión cuyo ejercicio afecta tanto a intereses corporativos generales como a intereses públicos del conjunto de la sociedad española, colectivo en el que —además— la deontología profesional siempre ha sido una seña de identidad.

En este sentido, el Tribunal Constitucional ya se ha pronunciado acerca del alcance y exigibilidad de la normativa deontológica[2]. Así, en su Senten-

---

1 Actualmente en revisión.

2 STC 219/1989 de 21 de diciembre

cia de 21 de diciembre de 1989, ya señalaba, en su Fundamento Jurídico 5, que «… las normas de deontología profesional aprobadas por los Colegios profesionales o sus respectivos Consejos Superiores u órganos equivalentes no constituyen simples tratados de deberes morales sin consecuencias en el orden disciplinario. Muy al contrario tales normas determinan obligaciones de necesario cumplimiento por los colegiados, velando por la ética y dignidad profesional».

Sin perjuicio de las obligaciones legales y deontológicas que afectan a la abogacía, también se han desarrollado una serie de normas en las que se refleja esta obligación, intrínseca a la profesión de abogado, de protección y seguridad de la información. Así, por ejemplo, la Estrategia de Ciberseguridad Nacional, dedica su Objetivo III a las necesidades de sensibilización, respecto de la cual señala que las empresas deben ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores y la confiabilidad de los servicios que prestan. Todo ello tendente a lograr la mejor protección de la confianza del consumidor, pues se considera que ello permitirá alcanzar el éxito de la economía digital.

Y para ello, la ECSN considera que debe promoverse *una sólida cultura de ciberseguridad, que proporcione a todos los actores la conciencia y la confianza necesarias para maximizar los beneficios de la Sociedad de la Información y reducir al mínimo su exposición a los riesgos del ciberespacio, mediante la adopción de medidas razonables que garanticen la protección de sus datos, así como la conexión segura de sus sistemas y equipos. La gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.*

También el Objetivo IV, dedicado a la sensibilización sobre los riesgos del ciberespacio, incluye una serie de elementos que nos sirven para fundamentar la obligación de diligencia y responsabilidad que, en materia de ciberseguridad, afecta a la abogacía. Dentro de este objetivo se destaca la necesidad de que las empresas tomen conciencia de la responsabilidad que tienen en la seguridad de los sistemas informáticos que utilizan, y de la protección de la información de sus clientes y proveedores. Y, para ello, la Estrategia apuesta por la promoción de una sólida cultura de ciberseguridad que sirva para mantener la confianza del consumidor. Dice así este Objetivo:

> *[…]*
> *Por tanto, una función esencial es promover una sólida cultura de ciberseguridad, que proporcione a todos los actores la conciencia y la confianza necesarias para maximizar los beneficios de la Sociedad de la Información y reducir al mínimo su exposición a los riesgos del ciberespacio, mediante la adopción de medidas razonables que garanticen la protección de sus datos, así como la conexión segura de sus sistemas y equipos. La gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.*

Para alcanzar estos Objetivos, la Estrategia se articula en una serie de líneas de actividad, en las cuales se recogen una serie de objetivos a lograr, de entre los cuales varios afectan a la profesión de abogado con mayor o menor intensidad. En particular, la Línea de Acción 4, que lleva por título "Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia", recoge en su último párrafo el compromiso del Gobierno de impulsar una serie de acciones dirigidas a asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado. En este sentido, se destaca la importancia de fomentar una eficaz cooperación con el Consejo General del Poder Judicial, la Abogacía del Estado, la Fiscalía General del Estado, la Fiscalía Coordinadora de la Criminalidad Informática y el Consejo General de la Abogacía Española.

Por su parte, la Línea de Acción 6, dirigida a la capacitación de profesionales contempla las iniciativas que es necesario acometer para alcanzar y mantener el adecuado nivel de capacitación en ciberseguridad de los profesionales (conocimientos y competencias) e impulsar la industria y la I+D+i españolas. En este sentido, la Estrategia fija como objetivo el desarrollar un marco de conocimientos de Ciberseguridad en los ámbitos técnico, operativo y jurídico.

Finalmente, la Línea de Acción 7, dedicada a fomentar la cultura de la ciberseguridad, incluye una serie de acciones dirigidas a concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

2. LOS CIBERRIESGOS EN LA ABOGACÍA Y SU GESTIÓN

En lo que respecta a la Abogacía Española, varios han sido los casos en que un despacho de abogados se ha visto afectado por un incidente de ciberseguridad. Según datos del INCIBE-CERT, en 2016 se gestionaron 70 incidentes por *ransomware* que afectaron a este tipo de organizaciones. Se detectaron 66 páginas web de despachos de abogados que habían sido infectadas con malware inyectado, y 158 habían sido víctimas de una alteración de su apariencia original (*defacement*). Mientras que 40 webs de despachos alojaban *phishing*.

Ciberseguridad y abogacía son dos conceptos que deben ir siempre unidos. De hecho, debería poder afirmarse que la ciberseguridad está siendo un elemento transformador del ejercicio de la abogacía. Y lo es porque está cambiando la tradicional organización y funcionamiento de los despachos y de los colegios, pero también del abogado en su condición de usuario de internet y de profesional del Derecho.

Así lo demuestra el hecho de que el Plan Estratégico para 2020 del Consejo General de la Abogacía Española haya incluido una medida específica a la ciberseguridad (94), en los siguientes términos:

> *94. Programa de ciberseguridad para Colegios, despachos y comunicaciones entre abogados: La profesión de abogado es definida, en gran medida, por la relación de confianza entre abogado y cliente. Por ello, el secreto profesional es fundamental para realizar la labor de defensa en una época como la actual en que los ataques a la seguridad de las redes de información transforman la protección de las comunicaciones de los abogados en una obligación para el Consejo y los Colegios de Abogados. La Abogacía Española elaborará un programa para abordar la problemática de la seguridad digital en el sector. En este sentido, promoverá el uso de estándares, tales como la metodología ENS-ISO 27001, así como programas de concienciación y protección frente a ciberataques, en colaboración con otras entidades públicas o privadas, e incrementando la coordinación con el Instituto Nacional de Ciberseguridad (INCIBE) así como el Centro Criptológico Nacional, y sus equipos de respuesta ante emergencias informáticas (CERT).*

Bien es sabido que son numerosos los riesgos a los que se enfrenta cada día un despacho de abogados, que ponen en peligro la información que maneja y custodia y, por lo tanto, son situaciones que pueden causar daño del que pueda derivarse algún tipo de responsabilidad legal.

La existencia de tales amenazas obliga a estas organizaciones a implantar, de manera efectiva y eficaz, una serie de medidas técnicas y organizativas, tanto de carácter preventivo como reactivo, a través de las cuales se traten de impedir, o en su defecto minimizar, los impactos negativos que pueda provocar un incidente de seguridad cibernético. Estos posibles im-

pactos van desde daños en el negocio hasta daños reputacionales de, en ocasiones, imposible reparación[3].

En cualquier caso, una ayuda para lograr este objetivo es la implementación de la norma técnica ISO 27000, la cual describe cómo gestionar la seguridad de la información en una empresa —o despacho de abogados— para poder reducir el riesgo de pérdida, robo o corrupción de información.

El legislador, conocedor de esta situación, ha incluido esta obligación en la regulación aplicable a la protección de la información. Véase, por ejemplo, el artículo 24.1 del Reglamento General de Protección de Datos cuando, al referirse a la responsabilidad del responsable del tratamiento, afirma que *el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.*

Mención esta que repite en los artículos 25.1 y 25.2 cuando se refiere a la protección de datos desde el diseño y por defecto; en el 28.1 y 28.4 cuando se refiere a la responsabilidad del encargado del tratamiento; o en el artículo 30 cuando regula el Registro de actividades del Tratamiento. Así como en otros artículos de la norma. Aunque, en este sentido, posiblemente la redacción del artículo 32.1 represente con mayor claridad cuál es el espíritu del legislador en materia de la protección de la información personal:

> *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
> *[…]".*

En España, esta exigencia se ha visto igualmente reflejada en el artículo 28.1 y otros de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, a través de la cual se completa lo dispuesto en el Reglamento antes citado.

---

[3] https://www.elperiodico.com/es/internacional/20180314/cierra-el-bufete-mossack-fonseca-epicentro-de-los-papeles-de-panama-6690712

En el ámbito general de la protección de la información, los artículos 14 y 16 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (comúnmente conocida como Directiva NIS) también recoge esta obligación de implementación de medidas técnicas y organizativas dentro de las organizaciones que tengan la consideración de operadores de servicios esenciales o de proveedores de servicios digitales.

Dicha obligación se refleja en la ley española que transpone al ordenamiento interno la citada Directiva NIS, en particular en el artículo 16 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Pues bien, de cara a poder identificar cuáles son los objetivos (de carácter cumulativo) que las medidas de ciberseguridad antes referidas deben lograr en lo que respecta a los despachos de abogados, podemos señalar principalmente cuatro: a) la confidencialidad; b) la integridad; c) la disponibilidad de la información; d) la autenticidad.

a) La confidencialidad de la documentación: esto es, las medidas de protección que se implementen por parte del despacho deben ir dirigidas a garantizar que la información sólo está accesible para aquellas personas que hayan sido autorizadas para ello.

   Desde un punto de vista organizativo, la protección de la confidencialidad puede organizarse de manera que, por un lado, se haga una buena gestión de identidades, es decir, que se configure adecuadamente los permisos de acceso a la información, en el sentido que se disponga de alguna solución que permita garantizar que los usuarios acceden únicamente a donde deben hacerlo (lo que se conoce como "principio de mínimo privilegio"). Y, de otro lado, debe garantizarse la eficacia de esta estructura a través de la realización de auditorías y controles periódicos, que permitan confirmar que tal diseño funciona adecuadamente.

   Además de este tipo de actuaciones, es recomendable que el despacho disponga de una política interna sobre rotación de contraseñas y diseño robusto de las mismas, además de que —entre otras medidas— se exija actualizar obligatoriamente los equipos tan pronto como esté disponible tal actualización por parte del proveedor, pues eso reduce el riesgo de sufrir un incidente conocido. Y todo ello, claro está, sin perjuicio de cualesquiera otras exigencias que puedan

venir derivadas de sistemas de gestión (SGSI) y calidad (ISO) que tenga implementados la organización.

En una vertiente más técnica, en lo que respecta a la protección de la confidencialidad puede destacarse el cifrado de la información como instrumento, en principio, eficaz para evitar accesos inconsentidos por parte de terceros ajenos a la organización. No obstante, téngase en cuenta que la eficacia de este instrumento siempre dependerá de la robustez del algoritmo de cifrado, por lo que se aconseja utilizar herramientas confiables y, en todo caso, una versión actualizada. En la práctica cabe destacar la proliferación de uso de redes VPN con las que conectarse remotamente a los sistemas de la empresa de una manera respetuosa con la confidencialidad de la información con la que se trata en la organización, bien sea del correo electrónico o de otro tipo de información.

b) La integridad de la información: que supone que las medidas de protección empleadas deben asegurar que la información permanece inalterada, tal y como el emisor la originó, sin manipulaciones externas.

   A estos efectos, existen en el mercado diferentes recursos tecnológicos con los que reforzar la seguridad perimetral de los sistemas que alojan información, y que permiten reforzar su seguridad frente a injerencias externas. Es el caso de los denominados Sistemas de Prevención de Intrusos (IPS) o de Detección de Intrusos (IDS).

   O los más conocidos Firewalls o Antivirus. Adicionalmente, una medida eficaz lo constituye el uso de *sand box* con el que ejecutar en un entorno seguro y previo, los ficheros que se reciben en el correo de la organización, pues reduce la posibilidad de que acceda a los sistemas un archivo potencialmente malicioso.

c) Disponibilidad de la información: de manera que la información esté accesible cuando se requiera.

   Para ello, una opción es la de diseñar los equipos y la arquitectura de la red del despacho de manera que pueda accederse a la información desde varias ubicaciones, para el caso de que por algún motivo el acceso principal estuviera inutilizado, lo que comúnmente se conoce como “redundancia”.

   Sí es una exigencia clara la de mantener la información de cuyo almacenamiento y custodia es responsable el despacho. Para ello será imprescindible realizar copias de seguridad periódicas (*back ups*) de un modo que se garantice la integridad y la disponibilidad de esa

información en el caso en que la información alojada en los sistemas principales se haya visto afectada, manteniendo una copia en un sistema distinto y aislado del principal, que actúe como centro de contingencia. En caso contrario podemos encontrarnos con que la incidencia que afecta al sistema principal (pe. Un ataque por ransomware), afecte de igual manera a la copia de seguridad, lo que haría ineficaz tal práctica.

d) La autenticidad.

En este caso, lo que se pretende es garantizar que la información a la que se accede es veraz, y que el transmisor de la información verdaderamente es quien dice ser.

Y es que para un despacho de abogados, tener la certeza de que la información que se recibe es verdadera, y que su remitente es el cliente, y no un tercero, es fundamental para poder proteger adecuadamente el derecho de defensa.

Este aspecto debemos ponerlo en relación con una de las amenazas, que se encuadran dentro de las que se conocen como "amenazas híbridas" y que son las noticias falsas (*fake news*), también referidas como "desinformación".

En efecto, en la actualidad están siendo los ataques dirigidos a influenciar a la opinión pública una de las amenazas que provocan mayor preocupación en la opinión pública. La difusión de noticias falsas puede afectar tanto a la situación de nuestro cliente como a alguno de los miembros del despacho o al propio despacho en sí. En este caso, mediante una actuación coordinada y utilizando los recursos de Internet, un tercero malintencionado difunde, de manera rápida y masiva, información falsa que afecta o puede afectar a algún hecho relacionado con el expediente que lleva el despacho, o a la reputación del cliente, de la propia organización o de alguno de sus abogados.

3. LOS INCIDENTES DE CIBERSEGURIDAD COMO AMENAZAS A LA DEONTOLOGÍA PROFESIONAL DE LA ABOGACÍA

El informe del Centro Criptológico Nacional sobre ciberamenazas y tendencias de 2018[4], destaca algunas que impactan directamente en la ac-

---

[4] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18 ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018.html

tividad de la abogacía. Por poner sólo algunos ejemplos y categorizar la tipología de los principales riesgos cibernéticos a los que se enfrenta la profesión, podemos citar los siguientes:

3.1. La suplantación de identidad

A través de esta práctica, un tercero crea uno o varios perfiles falsos con el objetivo de hacerse pasar por alguno de los integrantes del despacho, o por el propio despacho, con propósitos ilícitos.

Entre dichos fines podemos destacar el de acceder a información confidencial del despacho o de sus clientes, que se puede conseguir a través de técnicas de ingeniería social, como puede ser el comúnmente conocido como *phishing*[5], que consiste en remitir una comunicación electrónica con la apariencia de tener un origen lícito, en el sentido de que proviene del despacho o de alguno de sus abogados para, aprovechándose de esa apariencia de veracidad, ganarse la confianza del destinatario, quien facilitará los datos y credenciales que persigue el cibercriminal)[6]; o el *pharming* (mediante manipulaciones técnicas, el usuario es redirigido a una página web fraudulenta que suplanta a la oficial del despacho).

En relación con lo anterior, los despachos de abogados comienzan a ser víctimas del conocido como "fraude del CEO", en el que un empleado del despacho recibe una comunicación electrónica desde, presuntamente, uno de los socios, en la cual se le dan una serie de indicaciones para que, o bien realice algún tipo de transferencia económica o revele algún tipo de información confidencial, o bien haga *click* en un fichero o enlace malicioso que permita al cibercriminal acceder a los sistemas del despacho[7].

En este tipo de situaciones, la prevención es la mejor solución[8]. Una correcta formación a los empleados junto con protocolos internos de actuación, permitirán minimizar el riesgo de que los miembros del despacho sufran un engaño de esta naturaleza, lo que evitará sufrir daños. En este sentido, Google ha publicado la web *phishingquiz* en la que, a través de un

---

5 https://support.google.com/websearch/answer/106318?hl=es

6 https://www.incibe.es/protege-tu-empresa/blog/phishing-no-muerdas-el-anzuelo

7 https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-fraude-del-ceo

8 https://phishingquiz.withgoogle.com/

formato tipo cuestionario, enseña a los usuarios a identificar y neutralizar esta amenaza.

3.2. Infección de los sistemas del despacho por Malware

No disponer de suficientes medidas de seguridad para evitar que los sistemas del despacho puedan verse afectados por virus o software malicioso, facilita que aquel se vea expuesto a amenazas que pueden resultar más o menos dañinas para el negocio, pues pueden ir desde la instalación inconsentida de software con capacidad de interrumpir la normal actividad de los ordenadores del despacho (pe. Instalación de *adware*), hasta la entrada de software con capacidad de provocar daños más severos, tales como la instalación de troyanos o *spyware*, a través del cual un tercero ajeno a la organización pueda tener acceso inconsentido a información confidencial del despacho y de sus miembros, o incluso modificar la documentación a la que acceda. O de *keyloggers*, que permiten a un tercero acceder a la información que teclea el terminal infectado, por lo que se puede obtener información sobre comunicaciones (pe. De mensajería instantánea), contraseñas, números de cuenta, etc.

Dentro de esta categoría podemos destacar ciertas actividades ilícitas, las cuales, aprovechándose de determinadas vulnerabilidades técnicas, modifican la configuración original del blog o de la página web de un despacho para insertar de manera inconsentida e indeseada, mensajes o imágenes críticos con ese despacho o, incluso, amenazadoras (comúnmente conocido como *defacement*). Tenemos ejemplos de organizaciones o individuos que, para mostrar su disconformidad con una determinada política del despacho (caso de grupos denominados "hacktivistas"), o por razón de los clientes a los que defienden, tratan de mostrar su desacuerdo a través de esa vía.

Uno de los supuestos más habituales en la actualidad de infección por malware tiene que ver con las *botnet* o redes de ordenadores zombies, que son controlados por un tercero a través de lo que se conoce como panel de comando y control, desde el cual pueden manipularse los sistemas afectados y conseguir que desde la conexión del despacho (en particular a través de la dirección IP desde la que se conecta a Internet) un tercero pueda realizar ataques coordinados de denegación de servicio a otras instalaciones.

Dentro de la categoría de malware debemos incluir el ransomware, entendida como software malicioso que cifra el disco duro del terminal afectado, de manera que su legítimo usuario no puede acceder a ella. En este

caso el cibercriminal responsable del secuestro de información solicita un rescate para entregar la clave de descifrado y poder, así, recuperar el acceso a los ficheros donde se aloja la información del despacho[9].

Este malware ha tenido como máximo exponente el virus wannacry detectado el 12 de mayo de 2017, o el NotPetya, que cifraban los ficheros de todos aquellos terminales que sufrían una vulnerabilidad determinada. Este ransomware supuso una grave amenaza que afectó a los sistemas de innumerables despachos de abogados y causó daños por valor de miles de Euros, además de obligar a la paralización de sus actividades[10].

Dada la complejidad técnica que ofrecía este formato, recientemente ha comenzado a producirse una modalidad, que se ha denominado *cryptohacking*, mediante el cual lo que provoca la instalación de ese software malicioso no es el secuestro de la información, sino de la capacidad de computación del CPU, que pasa a utilizarse para el minado de criptomonedas a favor del ciberdelincuente.

3.3. Ataque de denegación de Servicio (DdOS)

También son habituales los ataques de denegación distribuida de servicio, o ataques DdOS, consistentes en un conjunto de técnicas que, mediante el envío de peticiones masivas al servidor consiguen saturar su capacidad de respuesta, dejándolo inoperativo.

Con ello se consigue la interrupción del funcionamiento normal del servicio, lo que en el ámbito de la abogacía puede afectar a las capacidades para elaborar o presentar documentos por vía telemática.

4. LAS AMENAZAS A LA DEONTOLOGÍA PROFESIONAL DEL ABOGADO

En el año 2013, la American Bar Association hizo pública una Resolución, que ha servido de base para una progresiva modificación del resto de códigos deontológicos de los colegios de abogados estadounidenses.

---

9 SAN de 3 de marzo de 2016. Id Cendoj: 28079220042016100012

10 https://cincodias.elpais.com/cincodias/2017/06/29/legal/1498730901_982733.html

Tal Resolución, fundamentada en un estudio del año 2012[11], introdujo una serie de cambios interpretativos y, en ocasiones, adaptaciones terminológicas, derivadas de la necesidad de que los abogados adaptasen su práctica profesional a unos nuevos tiempos dominados por la tecnología. De entre tales cambios destacamos dos, especialmente relevantes e ilustrativos para el caso que aquí nos ocupa.

El primero se refiere a la necesidad de que el abogado asesore adecuadamente a su cliente, obligándole a tener la formación y conocimientos suficientes para una correcta representación de aquel.

Esta obligación ya viene recogida en el código deontológico español, aunque la ABA le da una interpretación más amplia. Esto es, que respecto de la obligación de mantenerse continuamente formado y permanentemente actualizado, se exige que el abogado esté al corriente de los cambios en la ley y en su aplicación, incluyendo las ventajas y los riesgos asociados con la tecnología:

> *"to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology […]".*

El segundo de estos aspectos tiene que ver con la obligación para los abogados de proteger eficazmente la confidencialidad de la información de sus clientes, y que en dicho código se exige de la siguiente manera:

> *"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client".*

Dentro de esta última, la ABA considera que la exigencia de que los esfuerzos sean "razonables" incluye la utilización de instrumentos tecnológicos que garanticen la seguridad de esa información, así como la posibilidad de que los propios clientes puedan exigir, en determinados casos, un refuerzo en las medidas de seguridad implantadas, a tenor del grado de confidencialidad de la información tratada.

Estas adaptaciones éticas denotan la necesidad de interpretar los códigos deontológicos conforme a la realidad de estos nuevos tiempos, donde la tecnología es un elemento esencial en la práctica diaria de los profesionales, e Internet se ha convertido en el ecosistema habitual en el que

---

[11] https://www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on–ethics-20-20/.

los abogados prestan sus servicios y se comunican con sus clientes y con la administración de justicia.

En lo que respecta a la abogacía española, el nuevo Código Deontológico de la Abogacía, aprobado por el Pleno del Consejo General de la Abogacía Española en fecha 8 de marzo de 2019, introduce un nuevo artículo 22 bajo el título "empleo de las tecnologías de la información y la comunicación", en cuyo apartado 2 señala que "se debe hacer un uso responsable y diligente de la tecnología de la información y la comunicación debiendo extremar el cuidado en la preservación de la confidencialidad y del secreto profesional".

En lo que ahora nos ocupa, cabe destacar la referencia a la responsabilidad y diligencia en el uso de estas herramientas, así como el reconocimiento a la necesidad de extremar las precauciones con el fin de garantizar el respeto del secreto profesional, que el Código desarrolla en el artículo 5.

Aunque ya unos años antes, concretamente el 24 de marzo de 2009, la normativa de la Abogacía catalana era pionera en la regulación de esta situación, refiriéndose a este nuevo escenario, el artículo 9 de la Resolución JUS/110/2019, de 22 de enero, de modificación de la Normativa de la Abogacía Catalana del Consejo de los Ilustres Colegios de Abogados de Cataluña[12], completó el artículo 9, que lleva por título "nuevas tecnologías de la información y la comunicación", y al apartado 1, que señala que *los colegios de la abogacía en Cataluña y el Consejo promueven la correcta utilización de las nuevas tecnologías de la información y de la comunicación por parte de los profesionales de la abogacía*, se le añade un apartado 4, con la siguiente redacción:

> *4. Los colegios y el Consejo velan, en todo caso, por el cumplimiento de las garantías de ciberseguridad en relación con su propia actuación, y las promueven en la actuación de los profesionales.*

Por el contrario, llama la atención la total omisión que a la tecnología (y obviamente a la ciberseguridad en particular, o a la seguridad en general) hace el Código Deontológico de la Abogacía europea (CCBE). Sólo en la carta de principios esenciales de la abogacía europea, aprobada el 25 de noviembre de 2006, incluye una alusión a la tecnología dentro del principio (g), dedicado a la competencia profesional. Y lo hace afirmando que *es obvio que un abogado no puede aconsejar o representar a su cliente sino ha recibido una formación adecuada. Actualmente la formación de post-grado (continuación y*

---

12 Diario Oficial de Cataluña, de 30-01-2019

mejora de la formación profesional) ha adquirido una importancia creciente como respuesta a los rápidos cambios sufridos en el Derecho y la práctica del mismo y los nuevos avances tecnológicos y económicos.

Si entramos en el análisis de riesgos concretos a los que puede enfrentarse la abogacía a la hora de gestionar los riesgos que surgirán en el desarrollo de su actividad profesional a través de las tecnologías, podemos centrarnos en los siguientes aspectos potencialmente amenazados desde el punto de vista de la ciberseguridad:

a) La independencia del abogado

La independencia en todas sus actuaciones es un derecho y un deber para el abogado, además de una exigencia del Estado de Derecho y del efectivo derecho de defensa de los ciudadanos, tal y como señala la Constitución española, y destaca el artículo 2 del código deontológico de la abogacía española, cuyo Preámbulo también le dedica una referencia, al calificarla de necesaria dentro de un Estado de derecho y exigir que la actuación del abogado esté exenta de presión o coacción de ninguna clase.

Esta independencia es la que permite asesorar y defender adecuadamente los legítimos intereses de los clientes, de manera que se hace necesario preservar aquella frente a cualquier tipo de injerencias externas a su labor. Para ello deberán realizarse cuantas acciones sean necesarias para evitar presiones o exigencias de cualquier tipo, así como de intromisiones de intereses ajenos, pero también de los propios.

En el campo que ahora nos ocupa, existen algunos riesgos relacionados con la ciberseguridad que pueden amenazar a la independencia del abogado, en el sentido de ser aptas para interferir en la libertad del profesional a la hora de defender a su cliente.

Dentro de esta categoría podemos considerar al *defacement* o a la difusión de noticias falsas como amenazas que afectan a la independencia del abogado, en tanto en cuanto el impacto que pueden provocar en su libertad de actuación puede ser de un impacto e intensidad lo suficientemente relevantes como para que verse limitada en el sentido al que se refiere el artículo 2.2 y 2.3 del Código Deontológico de 2019.

b) La confianza en el abogado

El artículo 4 del Código Deontológico de 2019 recoge la obligación para el abogado de no defraudar la confianza de su cliente, exigiendo de aquel una conducta profesional íntegra, honrada, leal, veraz y diligente.

La diligencia exigible, además de la obligación de no defraudar la confianza, son elementos que deben tenerse en consideración en aquellos casos en que el despacho pueda sufrir algún tipo de incidente de ciberseguridad que pueda poner en riesgo el nivel de confianza del cliente en el buen hacer del abogado.

Esta diligencia no se refiere única y exclusivamente a la práctica profesional del derecho como tal, sino que debe entenderse como una actitud que debe mantenerse también durante todas las fases de la relación que el abogado mantenga con su cliente. Así las cosas, el abogado deberá adoptar medidas de carácter técnico adecuadas para proteger dicha confianza (plan de gestión de riesgos, auditorías de seguridad periódicas, formación a empleados…), pero también de fomento de la reputación del despacho y del propio abogado.

En el aspecto técnico, el cliente confía en que la infraestructura tecnológica de su abogado es adecuada para mantener la documentación y otra información que le facilita, a salvo de incidentes de ciberseguridad que puedan poner en peligro la integridad y confidencialidad de dicha información. Así, un incidente provocado por un ataque dirigido a la disrupción de los sistemas del despacho puede revelar la falta de medidas de seguridad, o su insuficiencia, para evitar un ciberataque de esta naturaleza que provoque una crisis de confianza en el abogado.

También un *defacement* de la página web del despacho, o un ataque exitoso de denegación de servicio que suponga una interrupción de la actividad del negocio, o una infección por *ransomware* derivada de una práctica poco diligente de alguno de los miembros del despacho, o una infección de la IP del despacho que lo convierte en parte de una *botnet* desde la cual se puedan producir ciberataques a sus propios clientes, son supuestos que deben tratar de evitarse ya que suponen una clara y grave amenaza a esta confianza, que el Código Deontológico de 2019 exige que sea objeto de protección.

A estos efectos, es recomendable que el despacho implemente medidas de monitorización de sus marcas (muy especialmente de sus nombres de dominio) y de su imagen (y de la de sus integrantes) a los efectos de detectar lo antes posible situaciones de suplantación de identidad, de registro ilícito de nombre de dominio, o de cualesquiera otras situaciones de carácter exógeno que puedan poner en peligro dicha confianza. En lo que se refiere a elementos de naturaleza interna del propio despacho, es habitual que esa confianza se pierda como consecuencia de comportamientos desafortunados de los abogados del despacho a través de sus perfiles en

redes sociales (comentarios, fotos, opiniones…), por lo que resulta también recomendable el diseño e implantación de políticas internas de buen comportamiento en redes sociales (*netiqueta),* y gestión de la identidad y reputación digitales.

c) El secreto profesional

Posiblemente sea éste el principio que más afectado se haya visto por el uso generalizado de Internet y de los medios sociales.

Se trata éste de un aspecto que, derivado —como señala el artículo 5 del Código Deontológico— de los principios de confianza y confidencialidad, impone al abogado el deber y le confiere el derecho de guardar secreto respecto de todos los hechos o noticias que conozca por razón de su actuación profesional.

Tal obligación, lejos de detenerse en el ámbito personalísimo del abogado, se extiende a la esfera de su personal y de cualquiera otra persona que colabore con él en su actividad profesional, a los que deberá hacer respetar igualmente ese secreto.

El robo de terminales de comunicación y almacenamiento (USB, teléfonos móviles, etc.) o la instalación de malware de espionaje (*spyware*) suponen una clara amenaza al secreto profesional, ya que si no se han implantado medidas de seguridad adecuadas, un tercero podría tener fácil acceso a información sensible y confidencial del despacho y de sus clientes.

La introducción en el sistema informático del despacho de un *malware* del tipo troyano, va a tener como consecuencia la fuga de documentación e información confidencial del despacho (expedientes, datos contables, nombres de clientes, etc.). Las fugas de información se han convertido en una de las principales amenazas de presente para los despachos de abogados ya que el daño que provocan afecta muy intensamente a la confianza del cliente en su abogado, cuya reputación se ve seriamente perjudicada. Este tipo de situación ya se recoge en la nueva legislación, tanto el nuevo Reglamento europeo de protección de datos y la nueva Ley Orgánica española en lo que a las fugas de datos personales se refiere (*data breach*), como la Directiva NIS y el Real Decreto-Ley 12/2018 respecto a las fugas de información derivadas de un incidente de ciberseguridad, lo que ha llevado a establecer un sistema de notificación de dichos incidentes a los organismos competentes e, incluso, a los clientes afectados, hecho este que también podría llegar a deducirse como obligación deontológica a la vista

de lo que dispone el artículo 13 del Código Deontológico de 2019 (antiguo artículo 10.9.e) en relación al deber de informar al cliente de la evolución del asunto encomendado.

Adicionalmente a esta amenaza al secreto profesional y a la confianza del cliente, debe tenerse en cuenta que en no pocas ocasiones la fuga de información viene provocada o causada por uno de los empleados de la organización afectada (*insider*), lo que todavía hace más necesario poder acreditar que el despacho, en cuanto organización responsable de la información que custodia, ha implementado planes eficaces de protección de aquella, que le permitan afrontar un incidente de esta naturaleza y gravedad de manera preventiva y reactiva pero, sobre todo, eficaz y de conformidad con la normativa aplicable a este tipo de supuestos.

El secreto profesional también puede verse quebrantado como consecuencia de interceptaciones de comunicaciones electrónicas de las que sea responsable el despacho. Ante esta posibilidad, el cifrado de la información sensible del despacho es una solución técnica de fácil implementación, y de gran eficacia. Además, es una solución que ya viene recogida en los apartados 3 y 4 del artículo 17 del Estatuto de la Abogacía Española, cuando señalan lo siguiente:

> *3. Cuando un Abogado sea requerido para prestar sus servicios profesionales por este medio, deberá adoptar las medidas necesarias para garantizar el secreto profesional y obtener del cliente acreditación suficiente de su identidad y la restante información que le permita evitar conflictos de intereses y prestar el asesoramiento adecuado al solicitante de sus servicios.*
>
> *4. Las comunicaciones confidenciales deberán enviarse encriptadas y con firma electrónica segura, siempre que las circunstancias del cliente lo permitan.*

5. LA COBERTURA ASEGURADORA

En relación a este extremo, por todos es sabido que la actividad del abogado debe estar cubierta por un seguro de Responsabilidad Civil (aun cuando no sea obligatorio en todo el territorio nacional tener suscrito tal seguro, al no existir previsión legal expresa estatal en tal sentido, es indudable que un ejercicio responsable de la profesión implica de suyo que el abogado cuente con la pertinente cobertura).

Tal obligación también es un deber de carácter deontológico, por cuanto el artículo 21 del código deontológico de la abogacía española incluye, en su apartado 1, la obligación de tener cubierta su responsabilidad profesional en la cuantía adecuada a los riegos que implique.

Esto nos lleva a preguntar si el actual sistema asegurador que da cobertura a la actividad profesional de la abogacía es adecuado y suficiente a los riegos cibernéticos a los que la profesión se enfrenta, o si bien es necesario buscar cobertura adicional, a través de los conocidos como *ciberseguros*, que incluyan entre sus riesgos a cubrir, todos los ciberriesgos presentes en el desarrollo de la abogacía moderna, algunos de los cuales ya hemos apuntado en el presente artículo.

En todo caso, la contratación de una póliza de esta naturaleza viene siendo recomendad dentro del desarrollo de los planes de *compliance* de las organizaciones, sin perjuicio de que pueda ser considerada una buena práctica a los efectos de la responsabilidad social de la entidad que lo contrate.

6. CONCLUSIONES

Bien es cierto que muchas de estas amenazas tecnológicas logran su objetivo por culpa de una insuficiente protección o actualización de los sistemas informáticos empleados. De hecho, en ocasiones, hasta resulta inevitable sufrir un incidente de esta naturaleza, por las propias vulnerabilidades de los programas y de la tecnología empleada. Este sería el caso, por poner un ejemplo, de las denominadas vulnerabilidades de día cero o "zero days".

Pero para el resto de casos, la diligencia profesional exige haber implantado todos aquellos aspectos técnicos que resulten necesarios para impedir o, en su caso, minimizar un eventual incidente de seguridad que ponga en peligro toda aquella información que le sea facilitada al abogado por su cliente.

Además de la necesaria inversión en infraestructura que pueden requerir las medidas de carácter técnico, también resulta igualmente exigible la implementación de medidas organizativas a través de las cuales se forme y conciencie a los empleados del despacho en lo relacionado con los riesgos cibernéticos que amenazan a la información custodiada por el abogado. En la actualidad la iniciativa "protege tu empresa" desarrollada desde el Instituto Nacional de Ciberseguridad de España (INCIBE), es una iniciativa gratuita y de fácil acceso que ayuda a los despachos de abogados a cumplir con esta obligación de protección de la información, especialmente cuando los daños se derivan de malas prácticas de los empleados.

Por último, señalar que es cierto que cada vez son más los despachos que migran toda su información a la nube, con la expectativa de que su provee-

dor cumpla con todas las medidas de seguridad suficientes para proteger el secreto profesional, que se vería afectado en el caso de un eventual acceso inconsentido, o una fuga de información derivado de una vulnerabilidad que pudiera ser explotada por un tercero. Por eso es importante que, en estos casos se extreme la diligencia del profesional, y se exija, también por vía contractual, que el proveedor de *cloud computing* que contratemos nos garantice la protección de la información que vamos a almacenar en esos sistemas.

Finalmente, puede señalarse que a la vista de la nueva redacción del artículo 22 del proyecto de Código Deontológico, parece haberse perdido una gran oportunidad de regular de una manera completa y adaptada a la realidad presente y futura, los aspectos deontológicos de la utilización de la tecnología por parte de la abogacía española, pudiéndose considerarse un tanto insuficiente para atender a la rica problemática que presenta el uso de las tecnologías por parte de la abogacía española.