# Deber de capacitación tecnológica para los abogados: una especial consideración a la ciberseguridad y su vinculación con el secreto profesional del abogado
*(Informe 6/2019)*

**Sumario:** I. INTRODUCCIÓN: EL DEBER DE FORMACIÓN DEL ABOGADO. II. SOBRE SI EXISTE UNA OBLIGACIÓN DEONTOLÓGICA DE CAPACITACIÓN TECNOLÓGICA PARA LA ABOGACÍA. 1. La postura continental. 2. La postura norteamericana. III. LA SEGURIDAD DE LA INFORMACIÓN Y EL SECRETO PROFESIONAL. IV. LA CAPACITACIÓN DEL ABOGADO ANTE RIESGOS DE SEGURIDAD. 1. En Estados Unidos. 2. En España. 3. La experiencia escocesa. V. CONCLUSIONES.

## I. INTRODUCCIÓN: EL DEBER DE FORMACIÓN DEL ABOGADO

El artículo 40.2 de la Constitución Española contiene un mandato para los poderes públicos de fomentar una política que garantice la formación y readaptación profesionales.

En lo que respecta a la abogacía, el debate en torno a la necesaria formación continua y actualización permanente de conocimientos no es nuevo, aunque en estos últimos años ha vuelto a tomar fuerza gracias a la aparición de lo que se viene denominando "transformación digital" o "transformación tecnológica" de la abogacía. Este aspecto recupera este viejo debate acerca de la correspondiente necesidad de que los abogados se adapten a este nuevo escenario, donde la sociedad conectada en la que vivimos aporta nuevas exigencias de conocimientos a los profesionales, tanto jurídicos como a nivel de usuario.

Así las cosas, y en lo que respecta a la responsabilidad de liderar esta misión, se ha venido considerando que los Colegios de Abogados son los agentes idóneos para capacitar a los profesionales de la abogacía en todos los ámbitos y, como no, también en el de la tecnología. Así se puede deducir de lo que señala el artículo 5.j) de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, cuando reserva a estas entidades las funciones de organizar actividades y servicios comunes de interés para los colegiados, de carácter profesional, formativo, cultural, asistencial y de previsión y otros análogos, proveyendo al sostenimiento económico mediante los medios necesarios.

O, en este mismo sentido, la Sentencia del Tribunal Supremo de fecha 16 de julio de 2018, cuando, en referencia a la obligación de colegiación profesional, afirma que "[ ] el establecimiento por el legislador de la colegiación obligatoria para el ejercicio de una profesión conforme al art. 3.2 de la Ley 2/74, responde a una valoración y se justifica por un interés público de que su ejercicio se ajuste a las normas o reglas que aseguren tanto la eficacia como la eventual responsabilidad en tal ejercicio, para cuya efectividad se atribuyen al colegio las funciones de tutela del interés de quienes son destinatarios de los servicios prestados por los profesionales que lo integran […]".

En línea con lo anterior, el Estatuto General de la abogacía otorga a las instituciones colegiales las facultades de formación profesional permanente, entendiendo que dicha formación es uno de los fines esenciales de los Colegios de Abogados (art. 3), los cuales —según se indica— podrán organizar actividades formativas adecuadas para lograr dichos objetivos de capacitación (art. 4 letras g) e i)).

En este mismo sentido, la Ley 34/2006, de 30 de octubre, sobre el acceso a las profesiones de Abogado y Procurador de los Tribunales, insiste en la importancia de la formación práctica de estos profesionales. En efecto, en referencia a esta circunstancia, el Considerando III de dicha Ley afirma que, en tanto en cuanto se les considera colaboradores fundamentales en la impartición de justicia, la calidad del servicio que prestan redunda directamente en la tutela judicial efectiva que nuestra Constitución garantiza a la ciudadanía. Y por ello se exige que quede garantizada de forma objetiva su capacidad para prestar la adecuada asistencia jurídica, lo que en una sociedad conectada debe —sin duda— incluir unas habilidades tecnológicas suficientes para poder lograr ese objetivo.

Esta previsión encuentra también reflejo en la regulación de los aspectos deontológicos de la profesión. Así, el Preámbulo del Código Deontológico de la Abogacía (en su versión de mayo de 2019) también se refiere a este aspecto cuando dice que "debe tenerse siempre presente la alta función que la sociedad ha confiado a la Abogacía, que supone nada menos que la defensa efectiva de los derechos individuales y colectivos cuyo reconocimiento y respeto constituye la espina dorsal del propio Estado de Derecho".

No obstante estas previsiones normativas, sigue abierto el debate —no sobre la necesidad, que es clara— si no sobre el derecho de los profesionales de la abogacía a exigir (y, por consiguiente, la correspondiente obligación de que se les ofrezca) una formación específica determinada en,

de un lado, el manejo de las tecnologías y, de otro lado, en los aspectos jurídicos del uso derivado de la misma.

Una discusión de esta naturaleza y alcance no solo es clave para el futuro de la profesión, sino que debe abordarse con prontitud, ya que en la sociedad actual (calificada por los expertos como "sociedad 4.0") y, sobretodo, en la sociedad futura que está por venir, se espera de los abogados que dispongan de conocimientos técnicos y jurídicos adecuados para el correcto desempeño de su profesión y, en consecuencia, de la adecuada protección del derecho a la defensa (a lo que el Estatuto General de la Abogacía se refiere como "la aplicación de la ciencia y técnica jurídicas").

Dentro de este ámbito relativo a los aspectos formativos y de capacitación de la abogacía española, uno de los extremos a los que se concede mayor relevancia y, por tanto, sobre los que más se debate, es el que tiene que ver con la ciberseguridad de los despachos de abogados.

En efecto, fue a raíz de varios incidentes de ciberseguridad que afectaron a empresas prestadoras de servicios jurídicos (en particular las revelaciones que se produjeron en el caso conocido como el de los "papeles de Panamá", y poco después con el cierre del despacho responsable de la fuga de información que se produjo; y el ciberataque al despacho británico DLA Piper), cuando la abogacía internacional tomó verdadera conciencia de la importancia de proteger adecuadamente la información digital entregada por sus clientes, que se almacena y custodia en base a, entre otros, el principio de confianza que rige la relación abogado-cliente[1].

En España, esta preocupación ya se incluyó en la antigua Estrategia de Ciberseguridad Nacional de 2013, cuando en la Línea de Acción 4 se afirmaba que el Gobierno de España iba a abordar una serie de medidas dirigidas a lograr el objetivo de potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz. Entre ellas, destacaba, a los efectos que ahora nos interesa, la de *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, es especialmente importante la cooperación*

---

[1] https://www.abogacia.es/2016/04/26/10-preguntas-a-francisco-perez-bes-el-grado-de-concienciacion-sobre-ciberseguridad-de-los-bufetes-todavia-es-bajo/

*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.*

Cabe recordar que, fruto de la previsión ahí recogida, el Consejo General de la Abogacía Española y el Instituto Nacional de Ciberseguridad de España, suscribieron un convenio por medio del cual se sentaban unas bases de colaboración en el apoyo y difusión de acciones preventivas y reactivas en la abogacía. Asimismo, también esta materia se incluyó en el Plan Estratégico de la Abogacía Española 2017-2020, de manera que mientras que en su medida 37 se recoge un compromiso de formación del abogado en competencias técnicas y habilidades digitales, la medida 94 se centra específicamente en el desarrollo de acciones de capacitación en ciberseguridad[2].

En el año 2019, el Gobierno aprobó una nueva Estrategia Nacional de Ciberseguridad (ENCS), en cuyo Capítulo 3 ("propósito, principios y objetivos para la ciberseguridad"), se incluye un Objetivo II que lleva por título "uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso".

El citado Objetivo II de la ENCS se compone —asimismo— de varias líneas de acción, de entre las cuales destacamos, a los efectos que ahora interesan, la número 3, la cual está dedicada al refuerzo de las capacidades de investigación y persecución de la cibercriminalidad.

Esta línea de acción 3 tiene como objetivo principal el de garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio, lo que se persigue a través de una serie de medidas

---

[2] 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).

de acción concretas, de entre las cuales las números 5 y 7 están directamente relacionadas con las necesidades formativas y de capacitación de los abogados en ciberseguridad, como seguidamente procedemos a detallar:

En cuanto a la primera de las medidas de acción citadas (esto es, la número 5), ésta tiene por objetivo el procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, al objeto de que se les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.

Mientras que la segunda de las medidas mencionadas (esto es, la número 7) persigue asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

## II. SOBRE SI EXISTE UNA OBLIGACIÓN DEONTOLÓGICA DE CAPACITACIÓN TECNOLÓGICA PARA LA ABOGACÍA

### *1. La postura continental*

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ha reconocido un derecho a la educación digital.

En efecto, el artículo 83 de la norma señala, a los efectos que aquí interesan, lo siguiente:

*3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.*

*4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.*

En lo que respecta a la formación de los abogados, la Exposición de Motivos II de la antes citada Ley 34/2006, de acceso a la abogacía, ya re-

cuerda que la necesidad de una real y efectiva capacitación profesional de los abogados, en su condición de necesarios colaboradores en el ejercicio de la tutela judicial efectiva, ha sido una reivindicación constante de los representantes de esta profesión.

Atendido lo anterior, podemos afirmar que es cierto que las referencias que contiene esta Ley están pensadas para garantizar unas competencias mínimas acreditadas que permitan al titulado acceder al ejercicio de la profesión tras la superación de una prueba de conocimientos. Pero no es menos cierto que no excluyen las exigencias de formación en temas relacionados con el uso y el impacto de las nuevas tecnologías.

En particular debemos hacer mención especial al tema de las competencias en seguridad de la información. En este escenario, el profesional de la abogacía tiene unas obligaciones de protección de la información de su organización, reforzadas por una serie de obligaciones éticas que, como abogado, le aplican de forma obligatoria, entre las que destaca claramente la de la protección del secreto profesional.

En este caso, las actuaciones del profesional de la abogacía quedan encuadradas, en primer lugar, dentro de las propias de un estándar mercantil de diligencia de un ordenado empresario en la gestión de una actividad profesional o empresarial. De ahí que la actividad propia de un abogado deba estar respaldada por un seguro de responsabilidad civil que cubra las posibles contingencias derivadas de un inadecuado asesoramiento jurídico al cliente o de una mala praxis que le cause algún daño, entre lo que se encuentra —claro está— la pérdida, revelación o acceso inconsentido a la información confidencial de sus clientes.

En relación con esto último podría traerse a colación la reciente modificación del artículo 49 del Código de Comercio, que pasa a incluir una serie de obligaciones relacionadas con la información no financiera de determinadas organizaciones, entre las que destacan la referente a la gestión de riesgos, área ésta donde los riesgos informáticos son cada vez mayores en número, pero también en relevancia y complejidad. O la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que también incide directamente en las necesidades de protección de la información empresarial.

Pero volviendo al asunto que ahora nos ocupa, el artículo 42.2 del Estatuto General de la abogacía exige al abogado un deber de información consistente en actuar con diligencia y atenerse a las exigencias técnicas adecuadas a la tutela del asunto que le haya sido encomendado, permitién-

dole que se auxilie de colaboradores y otros compañeros, quienes —afirma el artículo— actuarán bajo su responsabilidad[3].

Aunque quizás sea en el ámbito deontológico europeo donde esta obligación de capacitación se recoja de una manera más clara: así, el artículo 5.8 del código de la abogacía europea (CCCB) exige que el Abogado mantenga actualizados y desarrolle sus conocimientos y competencias profesionales teniendo en cuenta la dimensión europea de su profesión.

En España este precepto ha encontrado reflejo en el Código Deontológico de la Abogacía Española publicado en mayo de 2019, cuyo Preámbulo afirma que *quienes ejercen la Abogacía sólo pueden encargarse de un asunto cuando cuenten con la capacidad adecuada para ejercer su asesoramiento y defensa de una manera real y efectiva, para incrementar constantemente sus conocimientos jurídicos y para solicitar el auxilio de los más expertos, cuando lo precise.*

Y, más concretamente, el artículo 12.B.4, en el que se ha introducido un principio de prudencia que parece inspirado en la exigencia de diligencia y honestidad del abogado a la hora de prestar su asesoramiento profesional a un cliente, lo que también se recoge en el Código Deontológico de la Abogacía Europea, cuando en su apartado 3.1.3 prohíbe que el abogado acepte encargarse de un asunto sin la cooperación de un Abogado competente al respecto si sabe, o debería saber, que carece de la pericia necesaria.

Dicho principio de prudencia se expresa de la forma siguiente: "no debe aceptarse ningún asunto si uno no se considera apto para dirigirlo, a menos que se colabore con quien lo sea, informando al cliente, con carácter previo, de la identidad del colaborador"[4].

A la vista de esta redacción, a nuestro juicio, la aptitud en la dirección del asunto no sólo se circunscribe a los conocimientos técnicos del abogado, sino que puede hacerse extensivo a aspectos organizativos y de infraestructura. Dicho de otro modo, la ausencia en el despacho de sistemas informáticos que incluyan un nivel mínimo de seguridad para garantizar una protección razonable de la información facilitada por el cliente en virtud de su naturaleza, puede considerarse un elemento que debe ser valorado

---

3 *2. El abogado realizará diligentemente las actividades profesionales que le imponga la defensa del asunto encomendado, ateniéndose a las exigencias técnicas, deontológicas y éticas adecuadas a la tutela jurídica de dicho asunto y pudiendo auxiliarse de sus colaboradores y otros compañeros, quienes actuarán bajo su responsabilidad.*

4 https://www.abogacia.es/wp-content/uploads/2019/05/Codigo-Deontologico-2019.pdf

por el abogado a la hora de aceptar, o no, el encargo del cliente. Y a esta conclusión se llega al entender que la carencia de tecnología adecuada para la gestión de los riesgos a los que se enfrenta el despacho en cada momento, puede poner en serio peligro los principios de independencia y de confianza recogidos en el código deontológico de la abogacía española (en sus artículos 2 y 4), amén del secreto profesional (artículo 5).

También, y en este mismo sentido, la Carta de Principios Esenciales de la Abogacía Europea incluye, como Principio (g) una afirmación según la cual un abogado no puede aconsejar o representar a su cliente sino ha recibido una formación adecuada.

Este Principio añade que la formación de postgrado es una herramienta importante de cara a permitir a la abogacía su adaptación a los nuevos avances tecnológicos, donde —de alguna manera— lo que se parece querer fomentar es la figura de la formación especializada como herramienta adecuada para lograr el objetivo antes descrito[5].

No obstante, de una lectura detenida de dicho precepto no parece poder concluirse que la Abogacía europea sostenga que es necesario desarrollar formación de postgrado específica centrada en exclusiva en los aspectos jurídicos de las nuevas tecnologías. Antes al contrario, la redacción dada por la citada Carta parece referirse a la oportunidad (que también podríamos entender como necesidad) de que la formación de postgrado del abogado incluya entre sus contenidos aquellos aspectos que se consideren necesarios para lograr unas competencias tecnológicas y jurídicas suficientes y adecuadas, con independencia del sector en el que se desarrolle dicha formación de postgrado.

Así pues, a la vista de las regulaciones anteriores, podemos concluir que tanto en el deber de diligencia profesional general como, en particular, de las exigencias deontológicas para la Abogacía, se deriva una obligación de formación y capacitación adecuada para poder prestar al cliente los servicios que demanda con la calidad exigible. Pero no es menos cierto que, tomando en consideración que las actuales actuaciones profesionales actuales tienen un alto componente tecnológico, los abogados deben adquirir unas mínimas competencias tecnológicas. Es decir, no se trata de capacitar a los abogados en conocimientos técnicos avanzados, sino de formarles en aquellos aspectos que, con carácter mínimo, se van a demandar

---

5 Aprobado en la Sesión Plenaria del CCBE el 25.11.2006.

a un profesional del Derecho para garantizar la diligencia profesional en sus actuaciones.

O, dicho con otras palabras, no se trata de convertir a todos los abogados en especialistas tecnológicos (o "ciberabogados" como en ocasiones se les ha calificado), sino de evitar que existan profesionales cuyas carencias y desconocimiento en el uso habitual y normal de la tecnología pongan en riesgo la calidad y el rigor profesional exigible a una práctica profesional, lo que algunos han denominado "analfabetismo digital".

En relación con lo anterior, si pudiéramos considerar al Derecho Digital como una rama del derecho en la que un abogado pudiera especializarse, podríamos aplicar el artículo 6.4 del código deontológico. Este artículo —recordemos— exige que cuando en una comunicación comercial de un abogado se incluya como argumento publicitario una mención a la especialización profesional en una determinada materia, deberá poder acreditarse la veracidad de tal extremo a través del cumplimiento de una serie de requisitos relacionados con una previa y suficiente formación y experiencia profesional.

En particular, dicho artículo se expresa de la siguiente manera:

*Las menciones que a la especialización en determinadas materias se incluyan en la publicidad deberán responder a la posesión de títulos académicos o profesionales, a la superación de cursos formativos de especialización profesional oficialmente homologados o a una práctica profesional prolongada que las avalen*

Evidentemente, este artículo trata de evitar que, desde el punto de vista publicitario y de promoción de la actividad del despacho, surjan profesionales de la abogacía que se presenten ante el público de los consumidores como expertos en determinadas disciplinas que, por su extrema novedad, complejidad técnica o falta de desarrollo suficiente en la sociedad, no pueda acreditarse un mínimo de competencias que garanticen el nivel de servicio que se espera o, por lo menos, cubrir las expectativas que las afirmaciones difundidas por ese profesional haya podido crear entre el público al que se dirigen o alcanzan. Nos referimos, por ejemplo, a aspectos tales como tecnologías disruptivas (comúnmente conocidas como *DisTech*), dentro de las cuales podemos, a día de hoy, incluir tales como la inteligencia artificial o los aspectos legales derivados de la tecnología cuántica; aunque también en otras materias que, aunque algo más desarrolladas, no es posible acreditar una formación o una trayectoria profesional relevante, como ha venido ocurriendo con, por ejemplo, la ciberseguridad o el blockchain.

## *2. La postura norteamericana*

En el año 2013, la American Bar Association (ABA) emitió una Resolución en la que se introdujo la necesidad de que la abogacía adaptase su actividad profesional a una nueva realidad social. En esta realidad, y en esto debemos coincidir con la opinión de nuestros colegas norteamericanos, Internet se ha convertido en el ecosistema habitual donde la industria (concepto este que incluye tanto a los propios despachos de abogados como a sus clientes) presta sus servicios y comercializa sus productos[6].

En la práctica y dentro de esta obligación de competente defensa y asesoramiento del cliente (norma 1.1), esta actualización de las normas de la ABA ha llevado a que 36 estados *hayan modificado sus reglas de comportamiento para incluir, como requisito exigible, la* capacitación tecnológica del abogado. Y lo hace dentro de la interpretación que la ABA considera debe darse al concepto *maintaining competence* que utiliza para referirse a la obligación del abogado de mantenerse actualizado, tanto técnicamente (esto es, en la aplicación del Derecho) como tecnológicamente (conociendo los beneficios y riesgos que ofrece la tecnología).

Dentro de las previsiones contempladas en la Resolución antes indicada, y en particular en lo relacionado con la obligación de que el abogado preste un asesoramiento adecuado a su cliente, destaca la relativa a la necesidad de tener la formación y conocimientos suficientes para una correcta representación de aquel. Y lo hace utilizando la siguiente redacción:

> *"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 […]".*

Esta postura de la abogacía norteamericana parece acertada y no hizo más que anticiparse a recoger una obviedad, como es la de que en tanto en cuanto la tecnología se ha convertido en un elemento esencial de la sociedad conectada, debe serlo también en la práctica diaria de la abogacía. No en vano desde hace ya algún tiempo venimos siendo testigos del inicio de un proceso de transformación digital de la Abogacía, en el cual estos profesionales vienen utilizando Internet para prestar sus servicios y a comunicarse entre ellos y con sus clientes (donde, por ejemplo, podemos destacar

---

6 https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf

la proliferación de aplicaciones, plataformas de abogacía colaborativa o *marketplaces* para abogados), pero también para relacionarse, por ejemplo, con la administración de justicia a través de su Sede Judicial electrónica.

En este caso, la inclusión de la referencia antes indicada pretende ser un recordatorio de que los abogados deben mantenerse al tanto de las evoluciones tecnológicas que pueden afectar a su ejercicio. Tal obligación, lejos de parecer de nuevo cuño, se presenta como parte de las obligaciones éticas generales consistentes en mantener un nivel de competencia profesional adecuado a las nuevas circunstancias del caso y necesidades del cliente.

## III. LA SEGURIDAD DE LA INFORMACIÓN Y EL SECRETO PROFESIONAL

Como afirmaba la Presidenta del Consejo General de la Abogacía Española, Dª Victoria Ortega, durante su intervención en el Senado Internacional de Colegios de Abogados, dentro de los actos del 60º Congreso de la Unión Internacional de Abogados (UIA) durante su sesión de 29 de octubre de 2016: "el secreto profesional constituye la esencia y el principio fundamental del derecho de defensa. Cualquier norma que pretenda suprimirlo o limitarlo implica una merma del derecho a la defensa y por consiguiente afectaría al propio Estado de Derecho. Y desde luego, ninguna Abogacía del mundo podría consentirlo".

Efectivamente, y así lo contempla el Código Deontológico, el secreto profesional constituye uno de los pilares fundamentales de la profesión de abogado[7]. Y, como no podría ser de otro modo, tal relevancia así también se recoge tanto en la Ley Orgánica del Poder Judicial (en adelante LOPJ) como en la normativa colegial.

Por otro lado, la seguridad de las comunicaciones se ha reconocido recientemente como un derecho digital protegido por el artículo 82 de la Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales

---

7 Perviven como valores fundamentales en el ejercicio de la profesión de abogado la independencia, la libertad, la dignidad, la integridad, el servicio, el secreto profesional, la transparencia y la colegialidad.

(LOPDGDD), cuando reconoce el derecho de los usuarios a la seguridad de las comunicaciones que transmitan y reciban a través de Internet[8].

Sin intención de profundizar en el análisis general de esta figura, al no ser el objeto principal de este informe, sí debemos recordar los preceptos concretos donde se regula el secreto profesional. Y es que en lo que a la ciberseguridad se refiere —entendida ésta en su sentido más amplio como es el de la seguridad de la información— la información que custodia el abogado es el activo principal sobre el que debe girar la obligación de secreto, y de la que se derivan la responsabilidad legal y deontológica de aquél llegado el caso de que tal protección fracase.

En efecto, en lo que a la normativa legal se refiere, el artículo 542.3 de la LOPJ (y con idéntica redacción el artículo 32.1 del Estatuto General de la Abogacía) obliga a los abogados a guardar secreto de todos los hechos o noticias de que conozcan por razón de su actuación profesional, estableciendo, asimismo, un nivel de protección tal, que permite al abogado negarse a declarar sobre los mismos.

En cuanto al alcance y límites del secreto profesional, el Prólogo del Código Deontológico de la Abogacía Española le dedica estas palabras:

*El secreto profesional y la confidencialidad son deberes y a la vez derechos que no constituyen sino concreción de los derechos fundamentales que el ordenamiento jurídico reconoce a sus propios clientes y a la defensa como mecanismo esencial del Estado de Derecho. Todo aquello que le sea revelado por su cliente, con todas sus circunstancias, más todo aquello que le sea comunicado por un compañero con carácter confidencial, deberá mantenerlo en secreto, salvo las situaciones excepcionales previstas.*

Así las cosas, podemos afirmar que el secreto profesional, en su doble dimensión como derecho y como deber, comprende cualquier confidencia y propuesta que el abogado reciba, durante su actuación profesional, por parte de su cliente, pero también de la parte adversa y de los compañeros. El alcance objetivo de este aspecto es el de incluir todos los hechos y documentos de que haya tenido noticia o haya remitido o recibido por razón de cualquiera de las modalidades de su actuación profesional, tal y como se encarga de señalar el artículo 5 del Código Deontológico de la Abogacía Española.

---

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE nº 294 de 6 de diciembre de 2018.

Asimismo, el secreto profesional ampara las comunicaciones y negociaciones orales y escritas de todo tipo, con independencia del medio o soporte utilizado; e incluye las comunicaciones que se remiten o reciben a o desde otro abogado, de manera que no puede ser facilitada al cliente ni aportada a los Tribunales ni utilizada en cualquier otro ámbito.

Huelga decir que, en la totalidad de los casos, el abogado será receptor de comunicaciones, documentos y archivos en formato electrónico.

No obstante, también cabe recordar que este aspecto del secreto profesional no es un ámbito ilimitado. Antes al contrario, existen excepciones a esta obligación, que se recogen en el artículo 5.3 del Código Deontológico. Se trata de, por ejemplo, aquellos casos en lo que así lo autoricen expresamente el remitente y el destinatario. O para aquellos otros supuestos en los que sea el remitente quien deje expresa constancia de que dichas comunicaciones no se sujetan al secreto profesional. Y también en otras circunstancias en las que pueda extraerse determinada información de la obligación de secreto profesional, como aquellos casos en los que la Junta de Gobierno del Colegio de Abogados pueda autorizarlo discrecionalmente, siempre que concurra causa grave y previa resolución motivada con audiencia de los interesados.

De igual modo, también otros artículos de la normativa colegial vinculan el secreto profesional a la obligación genérica de diligencia profesional que se espera de un profesional de la abogacía. Así, por ejemplo, podemos destacar entre otros el artículo 42.1 del Estatuto General de la Abogacía Española, que incluye una referencia a la obligación de la abogacía de cumplir la misión de defensa que le sea encomendada *con el máximo celo y diligencia y guardando el secreto profesional.*

Pues bien, es en relación a este extremo relativo a la exigencia de confidencialidad y diligencia en la custodia de la información que nos confiere el cliente, donde la ciberseguridad juega un papel relevante, tanto en lo que se refiere a la formación técnica del profesional de la Abogacía, como en el nivel de diligencia exigible y aplicado al caso concreto.

En lo que a estos elementos se refiere, el entorno digital, los riesgos y amenazas inherentes a aquel, son aspectos cuyo desconocimiento bien podría entenderse como una actuación que no se adecúa a los parámetros de diligencia exigible al abogado durante la fase de captación, almacenamiento y custodia de la información protegida por el secreto profesional. Situación que, por otro lado, también se ve afectada por la obligación deontológica de hacer 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, tal y como se incluye, por primera vez, en el Código Deontológico (art. 21.2).

Si comparamos este aspecto con lo que se prescribe para la abogacía norteamericana, otro de los aspectos que pueden destacarse a los efectos que ahora nos interesan, tiene que ver con la obligación explícita que se establece, para los abogados americanos, de proteger eficazmente la confidencialidad de la información de sus clientes. Este extremo se exige de la siguiente manera en la norma de conducta 1.6. ("confidentiality of information") de la citada American Bar Association, cuando en su apartado c) señala que:

*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.*

Como puede fácilmente observarse, la normativa deontológica norteamericana goza, en este caso, de mayor concreción que la genérica obligación de diligencia que contempla la normativa española al regular el secreto profesional. Es más, la ABA considera que el nivel de esfuerzo exigible para prevenir una fuga de información debe ser el "razonable" al caso y a la situación concreta ante la que nos encontremos, para lo cual se exige con carácter previo, un análisis inicial de los riesgos que amenazan a la información que el abogado pasa a custodiar.

Y para poder realizar, de manera eficaz, un adecuado análisis de riesgos, será imprescindible tener unos conocimientos mínimos de las amenazas que, en Internet, pueden poner en peligro la integridad, disponibilidad o confidencialidad de tal información. Sin ello no será posible aplicar las medidas preventivas y reactivas, tanto técnicas como organizativas, que requieran la protección de los datos que nos ofrece el cliente. Ni solicitar a un experto el asesoramiento adecuado en relación a los riesgos previamente identificados.

Sin embargo, este nivel de prevención va más allá en la Resolución de la ABA, la cual añade, además de la utilización de instrumentos tecnológicos que garanticen la seguridad de esa información, 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. Esta medida no hace más que reafirmar nuestra afirmación anterior en lo que se refiere a la necesidad de realizar un análisis previo dirigido a determinar el alcance de las medidas que deben implantarse, según el caso.

## IV. LA CAPACITACIÓN DEL ABOGADO ANTE RIESGOS DE SEGURIDAD

### *1. En Estados Unidos*

En el informe publicado por Hanover Research en el año 2015 se debatía sobre cuál debe ser el rol del abogado en la gestión de las ciberamenazas de sus clientes, que dicen así: "in the past, many companies believed that cybersecurity could be managed primarily by IT staff and risk management. While some may still hold that belief, the question has largely shifted from wheter lawyers should be involved in a company's cybersecurity efforts to when lawyers should become involved"[9].

Esta afirmación se refuerza al analizar el *NIST handbook* del Gobierno estadounidense, donde divide la gestión de la ciberseguridad en tres funciones: controles técnicos, controles de gestión y controles operativos. Y de lo que el informe anteriormente citado concluye que los abogados son parte esencial en la planificación de la ciberseguridad, pues el conocimiento de las leyes y de los procedimientos es esencial durante todas estas fases.

En fecha 1 de mayo de 2019, la comisión de ética profesional del Colegio de Abogados de Maine, emitió una resolución en la que analizaba cuáles eran las responsabilidades de un abogado en el caso de haber sufrido una fuga de información derivada de un incidente de ciberseguridad, basándose en la Opinión Formal nº 483, que la ABA emitió el 17 de octubre de 2018.

Al igual que afirma la ABA en su opinión, la Resolución a la que hemos hecho referencia sostiene, en primer lugar, que un abogado debe realizar "esfuerzos razonables" al objeto de evitar una fuga de datos ("lawyers should take reasonable efforts to avoid a data breach").

Esto nos lleva a concluir que, desde una óptica deontológica, los abogados deben aplicar las medidas preventivas adecuadas para evitar verse afectados por un incidente de ciberseguridad que desemboque en una brecha de información o en una fuga de datos personales. Pero, igualmente, debe proceder obligatoriamente a llevar a cabo una serie de actuaciones previstas tanto en la normativa legal como deontológica al objeto de minimizar el posible daño, así como de informar adecuadamente a terceros (clientes afectados y al regulador, principalmente) de determinados aspectos rela-

---

[9] Bodenheimer, David. How lawyers help meet cyberthreats. Hanover Research, 2015.

cionados con los riesgos de acceso inconsentido a tal información por parte de terceros no autorizados a ello.

La Resolución del Colegio de Maine iba más allá, y entra a valorar tres aspectos que considera fundamentales para poder clarificar el alcance de la responsabilidad deontológica del abogado en relación a los deberes de prevención ante un incidente de ciberseguridad ocurrido en su despacho: la capacitación tecnológica del abogado, la defensa del secreto profesional y la formación al resto de miembros del despacho.

En cuanto al primero de estos aspectos, la Resolución se refiere a la necesidad de que los abogados dispongan de una capacitación profesional tecnológica específica, afirmando que no hay excusa para lo que denomina "incompetencia tecnológica", entendido esto como una exigencia de que cualquier abogado tenga un conocimiento mínimo y básico, y unas competencias mínimas en la tecnología que se emplea durante el ejercicio de la abogacía.

En palabras literales de la Resolución, para que un abogado que actúa utilizando elementos tecnológicos pueda prestar un servicio competente debe tener *a baseline understanding of, and competence in, the technology used in the practice of law must be maintained by every lawyer.*

Como puede observarse (y así hemos mencionado anteriormente), las referidas exigencias no son una obligación de tener conocimientos tecnológicos profundos ni avanzados, sino tan solo suficientes para garantizar un nivel de competencia adecuado en la prestación de los servicios a sus clientes. En este caso, el Colegio de Abogados de Maine, al igual que los del resto de estados, diseñan este requisito de manera que sean los propios profesionales los que, en interés de su propia responsabilidad, cumplan con su obligación deontológica como abogado.

Partiendo de la postura del Colegio de Maine, el Colegio de Florida ha implementado un sistema obligatorio de actualización de conocimientos en el sentido de que cada 3 años todos los abogados ahí colegiados deben asistir a una formación de tres horas centrada específicamente en manejo de tecnología ("in approved technology programs")[10]. Esta iniciativa derivó de la modificación de la normativa colegial tras la sentencia emitida por la Corte Suprema de Florida, de fecha 29 de septiembre de 2016, en la que, tras la propuesta de modificación de la normativa interna del Colegio a ini-

---

[10] https://www.lawsitesblog.com/2016/10/florida-becomes-first-state-mandate-tech-cle.html

ciativa del Colegio de abogados de Florida (Florida Bar), ordena adaptar la normativa colegial a los principios sugeridos por la ABA, en este caso en lo relacionado con las competencias tecnológicas de los abogados, como hemos analizado anteriormente.

En segundo lugar, destaca la obligación de proteger el secreto profesional durante un incidente de ciberseguridad, de manera que si como consecuencia de un incidente de tal naturaleza (provocado por un ciberataque o por cualquier otra circunstancia) se produjera una fuga de información (personal o no), la responsabilidad por no haber protegido adecuadamente la información del cliente recaería sobre el abogado.

Por último, el abogado debe formar y supervisar las actividades de los miembros del despacho en relación a sus obligaciones de salvaguardar la información del cliente ante riesgos que puedan dar lugar a su pérdida o a una revelación pública inconsentida.

### *2. En España*

En España, y dentro del ámbito de la protección de datos personales, podemos remitirnos a la obligación que recoge el artículo 28.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, donde el legislador establece como presupuesto básico en la protección de la información personal, el del principio de la responsabilidad proactiva.

Gracias a esta exigencia, corresponde a los responsables y encargados del tratamiento de datos de carácter personal, la implementación de aquellas medidas técnicas y organizativas apropiadas que sirvan para garantizar y acreditar que el tratamiento que hacen de dicha información es adecuado y conforme con la normativa sobre protección de datos.

La adopción de tales medidas, así como su efectividad, deberán ser acreditadas ante el regulador en el caso de que se hubiera producido alguna situación en la que haya tenido lugar algún tipo de fuga o pérdida de información personal.

Adicionalmente, en el caso de que algún despacho obtenga la certificación conforme al Esquema Nacional de Seguridad (ENS), debería cumplir con las exigencias que marca el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el cual también contempla la necesidad de formación.

### *3. La experiencia escocesa*

En 2019, la Law Society of Scotland, creó una acreditación a través de la cual los abogados escoceses y los paralegales reconocidos que puedan demostrar un nivel determinado de experiencia en la aplicación del derecho en el ámbito tecnológico ("legal technology"), puedan considerarse oficialmente expertos en esta materia[11].

Tal experiencia deberá ser acreditada, tanto a través de la experiencia profesional que pueda demostrarse, como a través de las publicaciones realizadas y de las recomendaciones que terceras personas hagan de ti. Y si el comité evaluador lo considera suficiente, se concede al profesional que lo solicite el reconocimiento de experto en esta materia.

Esta fórmula resulta interesante a los efectos de poder establecer un mecanismo que permita, a los que se presenten en el mercado como expertos en alguna de las materias que caen bajo el ámbito de lo que puede denominarse "derecho digital", a acreditar la veracidad de sus afirmaciones, lo que en España hemos visto cuando nos hemos referido a la prohibición establecida en el artículo 6.4 del código deontológico de la abogacía española, cuando se refiere a los límites de la publicidad de los abogados.

Siguiendo con las características de la iniciativa escocesa, la validez de la acreditación de la Law Society es de tres años, una vez transcurridos los cuales el especialista deberá obtener una nueva acreditación, previo el pago de 300 libras esterlinas y siguiendo el procedimiento establecido a tal efecto.

## V. CONCLUSIONES

Es importante tomar conciencia, y adaptar las normativas legales y deontológicas, a una realidad donde los clientes esperan, y tienen derecho, a que su abogado tenga conocimientos mínimos suficientes —por lo menos básicos— en las nuevas tecnologías, en el manejo de las mismas, así como de sus implicaciones jurídicas.

Dentro de las competencias formativas que ostentan los Colegios de Abogados, es recomendable que se incluyan itinerarios a través de los cua-

---

[11] https://www.lawscot.org.uk/members/career-growth/specialisms/accredited-legal-technologist/

les se ofrezca a los abogados colegiados formación en el uso de aquellas tecnologías que puedan tener impacto en el ejercicio habitual de la profesión, como puede ser la ofimática, uso de correo electrónico, y otros sistemas idóneos para poder ejercer la abogacía de manera eficaz y eficiente, pero sobre todo con seguridad.

También deben diseñarse y llevarse a cabo, por parte de los Colegios de Abogados y de sus Consejos, actividades continuas de concienciación y sensibilización en materia de ciberseguridad, protección de la información y gestión de riesgos tecnológicos, para dar cumplimiento a las previsiones recogidas en la Estrategia Nacional de Ciberseguridad, así como en la normativa legal y deontológica aplicables.

Deberá fomentarse el desarrollo de pólizas de seguro de responsabilidad civil adecuadas para los despachos de abogados, que cubran los posibles riesgos tecnológicos que puedan afectar al normal desarrollo de su actividad, tanto a nivel interno como en la relación con sus clientes.

Deberá potenciarse el desarrollo de buenas prácticas y de códigos de conducta que permitan a los despachos de abogados desarrollar políticas internas adecuadas en materia de protección de la información y ciberseguridad, que puedan, además, incardinarse dentro de sistemas de Responsabilidad Social Empresarial en los que aquellos puedan incorporarse, fomentando la adopción de sellos de calidad especialmente destinados a la gestión de riesgos y protección de la información (pe. ISO 27001, 19600, etc.).

Desde las instituciones colegiales deberá apoyarse la formación reglada universitaria (pe. Masters) así como sistemas de certificación que incorporen a su programa formativo itinerarios de capacitación de los profesionales de la abogacía en temas relacionados con la ciberseguridad (pe. Compliance, DPO, CISO ).