LA CIBERSEGURIDAD COMO DEBER DEONTOLÓGICO DEL ABOGADO: UNA MIRADA AL FUTURO DE LA PROFESIÓN

Autor: Jaime Sardina Tortosa

Resumen

Al hilo de la transformación digital de la abogacía, surge como reforma fundamental la actualización de su Código Deontológico al objeto de incluir la ciberseguridad como necesaria medida de prevención que proteja el ejercicio profesional de injerencias externas. Este trabajo tiene como fin aportar una propuesta regulatoria de la ciberseguridad como deber deontológico, para lo cual se atenderá a la regulación comparada en otras jurisdicciones, así como a los riesgos concretos que afectan a la profesión.

Abstract

To follow on from the digital transformation of the legal profession, it arises as a key reform the updating of its Code of Ethics so as to include cybersecurity as a necessary preventive measure to protect the professional practice from external interference. The purpose of this work is to provide a regulatory proposal for cybersecurity as a deontological duty, for which comparative regulation in other jurisdictions will be addressed, as well as the specific risks that affect the profession.

Palabras clave: ciberseguridad, deontología, abogacía, riesgos.

Keywords: *cybersecurity, deontology, advocacy, risks*.

Introducción

Pese al cariz innovador que inspira la temática del presente trabajo, permítame el lector el aparente anacronismo de traer a colación un postulado del insigne jurista Ángel Ossorio y Gallardo, escrito hace ya casi un siglo, pero cuyos fundamentos y advertencias resultan plenamente de aplicación en el cambiante y dinámico mundo en el que se desenvuelve el ejercicio actual de la abogacía: *lo que al Abogado importa no es saber el Derecho, sino conocer la vida. El Derecho positivo está en los libros. Se buscan, se estudian, y en paz. Pero lo que la vida reclama no está escrito en ninguna parte. Quien tenga previsión, serenidad, amplitud de miras y de sentimientos para advertirlo, será Abogado*[1].

Dicho postulado bien podría haber inspirado la carrera profesional de don Jose María Cervelló, pionero en el desarrollo de la abogacía internacional en España, y motivado la creación de la Cátedra que toma su nombre, la cual tiene como uno de sus objetivos el desarrollo de proyectos de investigación y la promoción del diálogo sobre temas de actualidad jurídica entre profesionales del sector, en un acertado y loable intento de despertar en el abogado actual el afán de anticipación a los problemas jurídicos de su tiempo, todo ello, como apuntaba Ossorio y Gallardo, en aras de conocer la vida y satisfacer las demandas y necesidades que reclama la sociedad actual.

Llegados a este punto, advierto con satisfacción cómo el planteamiento de un trabajo sobre la ciberseguridad y su relación con la deontología del abogado colma totalmente esas aspiraciones de previsión y actualización que promueve la Cátedra José María Cervelló, incentivando el conocimiento de la transformación digital que está afectando a la profesión de abogado y que, lejos de ser una amenaza, debe constituir una oportunidad para ofrecer un servicio más rápido, seguro y completo.

Si atendemos a la realidad de nuestro tiempo, resulta patente que la abogacía está incorporando las nuevas tecnologías de la información y la comunicación ("TIC") en su práctica profesional diaria. No obstante, resulta esencial que sepamos entender y

[1] Ossorio y Gallardo, A., *El alma de la toga*, Reus, Madrid, 2008, p. 29.

cumplir las obligaciones éticas que derivan de dichas TIC, especialmente en lo atinente a la competencia y confidencialidad del abogado, áreas de nuestra deontología que se están viendo más afectadas por los nuevos cambios tecnológicos.

De cara a presentar mi estudio sobre la materia, he creído conveniente comenzar con una necesaria aproximación a la regulación actual de la ciberseguridad en sede deontológica; para ello, y dado el carácter global y universal que plantea la ciberseguridad en la abogacía, ofreceré un pequeño análisis comparado, a fin de revelar cuál es la situación actual a nivel mundial y la posición de España en relación con el resto de jurisdicciones, lo cual permitirá discernir, en las conclusiones del trabajo, qué aspectos implantados en el extranjero pueden ser de interesante transposición a nuestro Código Deontológico.

Acto seguido, destacaré cuáles son los riesgos cibernéticos a los que se enfrenta hoy en día la profesión de abogado, de cara a conocer cuáles son los concretos incidentes de seguridad informática que nos pueden afectar y poder ofrecer, al final del trabajo, ideas y soluciones más precisas y eficaces con las que abordar el problema. Una vez realizada dicha exposición, abordaré los diversos deberes deontológicos actuales que se pueden ver afectados por este nuevo escenario tecnológico.

Por último, y sobre la base de todo lo anterior, detallaré una serie de propuestas tendentes a la regulación de la ciberseguridad en el Código Deontológico, así como diversas medidas y soluciones que todo abogado debería adoptar en su esfera personal para una mejor prevención y protección de sus sistemas y, en última instancia, de la información relativa a sus clientes.

Sirva, pues, este trabajo, dicho sea con la debida humildad de este joven abogado que suscribe, como un paso más en el empeño de incorporar la ciberseguridad como deber deontológico de la profesión.

Análisis comparado de la ciberseguridad en materia deontológica

España y la Unión Europea

Según el Indice Global de Ciberseguridad, elaborado por la Unión Internacional de Telecomunicaciones[2], organismo de la Organización de las Naciones Unidas especializado en telecomunicaciones, España ocupa en la actualidad el puesto 25º de Europa y el 54º del mundo en nivel de compromiso y desarrollo en materia de ciberseguridad. Esta posición no es especialmente satisfactoria si tenemos en cuenta que España es la 13ª economía del mundo en términos de Producto Interior Bruto[3], lo cual debería corresponderse, en teoría, con una posición equivalente en términos de ciberseguridad.

De hecho, obviando alguna previsión al respecto en el Código Penal[4], no existen en nuestro ordenamiento leyes ni requisitos aplicables a las organizaciones en general, sino solo algunas reglas dirigidas a colectivos concretos de empresas relacionadas con la ciberseguridad, como los proveedores de servicios de la sociedad de la información[5] o los operadores críticos responsables del funcionamiento de alguna infraestructura estratégica[6], siendo la regulación, por lo general, bastante dispersa, sectorial e insuficiente, comparada con la de otros países[7].

---

[2] International Telecommunication Union , "Global Cibersecurity Index (GCI) 2017", 2017, p. 57.

[3] Fuente: Banco Mundial. Disponible en: http://wdi.worldbank.org/table/4.2#

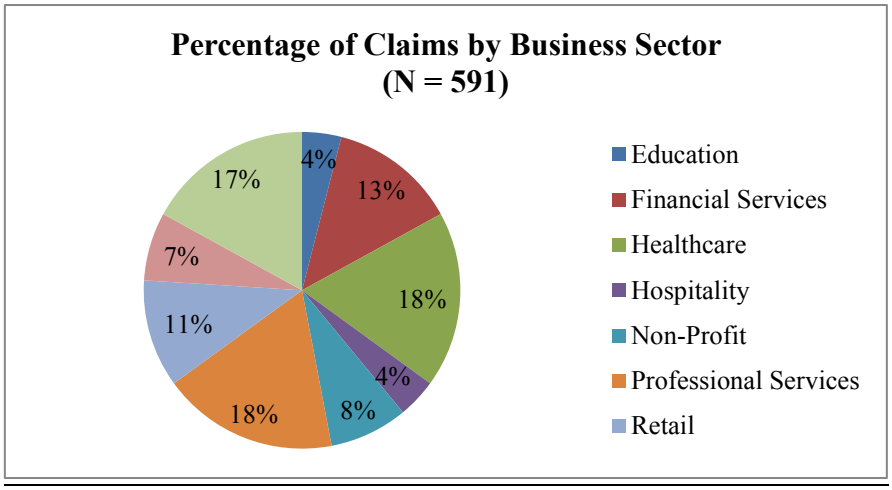
[4] El Código Penal fue modificado en 2010 para adaptarlo al Convenio sobre la Ciberdelincuencia y la Decisión Marco del Consejo 2005/222/JHA sobre ataques contra los sistemas de información.

[5] A través de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. En su disposición adicional novena, se establece la obligación de dichos prestadores de servicios, junto a los registros de nombres de dominio y los agentes registradores que estén establecidos en España, de colaborar con el Equipo de Respuesta ante Emergencias Informáticas competente ("CERT"), por sus siglas en inglés) en la resolución de incidentes de ciberseguridad que afecten a la red de Internet.

[6] A través de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. En su artículo 13 se establece la obligación de dichos operadores de, entre otras, asistir técnicamente al Ministerio del Interior, colaborar con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales o elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente.

[7] VV.AA., *The Privacy, Data Protection and Cybersecurity Law Review*, Law Business Research, 2016, pp. 318-319.

Descendiendo al caso concreto de los despachos de abogados, resulta preocupante la falta de previsión normativa al respecto, toda vez que el sector de servicios profesionales es el más afectado por los ataques cibernéticos. Concretamente, de acuerdo con el siguiente gráfico elaborado por NetDiligence, un 18% de los ataques cibernéticos tienen como objetivo este sector, por delante de sectores como la banca, la educación o la sanidad.



Fuente: NetDiligence[8].

Esta falta del debido nivel de desarrollo que España debería tener en materia de ciberseguridad se ve reflejada en la normativa deontológica de sus colegios de abogados, donde las referencias a la necesaria actualización de sus abogados en relación con las nuevas tecnologías que están transformando la profesión brillan por su ausencia.

Así, si atendemos al Código Deontológico de la Abogacía Española, no se encuentra referencia alguna a los nuevos avances tecnológicos, mucho menos al ámbito concreto de la ciberseguridad, debiendo entenderse que dicha labor de formación y adaptación a los nuevos escenarios que plantean las nuevas TIC se engloba dentro del deber genérico del abogado de ejercer su profesión con la debida competencia, tal y como prevé el preámbulo de dicho Código y se concreta en su artículo 13.8, sobre la relación con los clientes.

[8] NetDiligence, "2017 Cyber Claims Study", 2017, p. 16.

Si descendemos al ámbito autonómico, la escasez de referencias y alusiones a los nuevos desafíos tecnológicos es palmaria. La única Comunidad Autónoma que mantiene una previsión al respecto es Cataluña, a través de su Resolución JUS/880/2009, de 24 de marzo, por la que se inscribe en el Registro de Colegios Profesionales de la Generalidad de Cataluña la Normativa de la Abogacía Catalana, en cuyo artículo 9.1 se establece:

> *Los colegios de abogados catalanes y el Consejo de los Colegios de Abogados de Cataluña promoverán la correcta utilización de las nuevas tecnologías de la información y de la comunicación por parte de los abogados.*

Una vez visto el caso español, si analizamos los códigos deontológicos de otros países de la Unión Europea, se llega a la misma conclusión[9]; en ninguno de ellos se recoge una mención específica sobre los nuevos desafíos tecnológicos que deben transformar el ejercicio de la profesión y sus correlativas obligaciones éticas y deontológicas. Esta carencia a nivel europeo se comprende si acudimos al Código de Deontología de los Abogados en la Unión Europea, el cual no recoge ninguna previsión sobre la materia. Es más, en su capítulo específico sobre la formación de los jóvenes abogados, colectivo que tendrá que lidiar con total seguridad con los avatares de la transformación digital, únicamente se alude a la necesidad de conocer las leyes y normas procesales aplicables en los distintos Estados Miembros, lo que deja entrever el notable atraso y falta de actualización del Código en lo que a la transformación de la profesión se refiere.

Resto del mundo

No obstante lo comentado en el epígrafe anterior, existen otras jurisdicciones en el mundo, especialmente las de origen anglosajón, que ya han introducido previsiones en sus códigos deontológicos sobre la necesidad de que el abogado posea ciertos conocimientos tecnológicos para ser competente de cara a llevar determinados asuntos de su cliente.

[9] Para consultar los diversos códigos deontológicos de los países de la Unión Europea, puede consultarse la traducción al inglés de todos ellos en la página web del Consejo de la Abogacía Europea, accediendo al apartado "National Code of Conduct", en el siguiente link: https://www.ccbe.eu/documents/professional-regulations/

El paradigma en este sentido lo constituye Estados Unidos. En el año 2012, la American Bar Association promulgó una serie de reformas que actualizaban las normas deontológicas de la abogacía estadounidense para reflejar los deberes éticos del abogado en la nueva era digital[10]. Centrada en los principios de competencia y confidencialidad, el objetivo de la reforma era concienciar a los abogados que utilizan las nuevas tecnologías de la información para adoptar medidas efectivas y razonables que salvaguarden la información del cliente[11].

Las principales medidas adoptadas, en lo que al presente trabajo interesa, fueron las siguientes:

- **Competencia**: inclusión expresa de conocimientos tecnológicos en el deber de actualización que todo abogado debe observar para mantener su competencia técnica de cara al cliente.

  > *To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology</u>, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject*. [12]

- **Confidencialidad**: se especifica el deber de diligencia que debe mantener un abogado de cara a proteger la información del cliente frente a injerencias externas.

  > *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*. [13]

---

[10] "Resolution 105A, Commission on Ethics 20/20", American Bar Association, Abril 2012.

[11] Ries, D., "Cyber Security for Attorneys: Understanding the Ethical Obligations", *Law Practice Today*, Marzo 2012.

[12] Resolution 105A, Commission on Ethics 20/20, *op. cit.* p. 3.

[13] Resolution 105A, Commission on Ethics 20/20, *op. cit.* p. 4.

A la vista del espíritu de la reforma, esta previsión parece traer causa de los nuevos riesgos cibernéticos que amenazan la confidencialidad de la información ajena que un abogado posee con ocasión de la prestación de sus servicios a un cliente determinado.

Sobre la razonabilidad de las prevenciones adoptadas, que excluirían la responsabilidad del abogado, la propia Resolución indica como factores a tener en cuenta la importancia de la información, la probabilidad de revelación de dicha información si no se adoptan otras medidas, el coste de implementar esas medidas adicionales de seguridad, la dificultad de dicha implementación y el grado en que dichas medidas puedan perjudicar la habilidad del abogado para representar a su cliente (por ejemplo, porque el software o dispositivo utilizado sea excesivamente difícil de usar).

- **Derechos de terceras personas**: se recoge una nueva previsión sobre la recepción accidental de información en formato electrónico y la obligatoriedad de avisar al emisor al respecto para que adopte las medidas necesarias.

> *A lawyer who receives a document or electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender*[14].

Estas modificaciones no tienen carácter imperativo, sino que se establecen por la American Bar *Association* como directrices para los distintos colegios estadounidenses, los cuales son libres de incorporarlas a sus códigos deontológicos. No obstante su naturaleza orientativa, son ya 28 los Estados que han decidido recoger en sus códigos deontológicos una previsión sobre los necesarios conocimientos tecnológicos del abogado a la luz de la citada reforma[15].

---

[14] Resolution 105A, Commission on Ethics 20/20, *op. cit.* p. 5.

[15] Sobre los concretos Estados que han implementado estas modificaciones, véase el análisis de Robert Ambrogi, popular abogado estadounidense, escritor y consultor de medios, en su blog *Law Sites*:

Incluso algunos de los Estados que no han adoptado formalmente en sus códigos deontológicos las nuevas modificaciones propuestas por la American Bar Association, no han permanecido ajenos a dicha materia y han reflejado la importancia de atesorar conocimientos tecnológicos en circulares y opiniones.

En este sentido, especialmente explícito ha sido el Colegio de Abogados de New Hampshire, al integrar la debida competencia profesional en los siguientes términos:

> *Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes*[16].

De manera similar, el Colegio de Abogados de California transcribe prácticamente la nueva previsión de la American Bar Association:

> *Maintaining learning and skill consistent with an attorney's duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology*[17].

Por su parte, el Colegio de Abogados de Canadá, si bien no realiza en su código deontológico ninguna alusión concreta a la necesaria adaptación y capacitación del abogado en asuntos tecnológicos, sí ha elaborado varios informes de interés en los que se plantean ciertas recomendaciones de cara a la concienciación del abogado sobre las obligaciones éticas y profesionales que se derivan del uso de ciertas tecnologías. En uno de ellos, precisa que las medidas de seguridad a adoptar deben proteger la integridad, disponibilidad y confidencialidad de la información del cliente, sugiriendo al respecto las siguientes conductas[18]:

---

https://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html

[16] "Advisory Opinion 2012-13/4", New Hampshire Bar Association, 2012.

[17] "Formal Opinion nº 2015-193", The State Bar of California Standing Committee on Professional Responsibility and Conduct, 2015.

[18] "Legal Ethics in a Digital World", CBA Ethics and Professional Responsibility Committee, 2015.

- Para salvaguardar la integridad, se plantea el uso de firmas digitales, políticas especiales para el archivo de documentos, comparación de metadatos y limitación del uso de la firma electrónica por terceros.
- En relación con la disponibilidad, aconseja la realización regular de copias de seguridad, una revisión rutinaria que asegure que la información puede ser recuperada y la contratación de un seguro que cubra los costes de recuperación de información electrónica perdida.
- Para preservar la confidencialidad, se recomienda cerrar los armarios de archivo de información, restringir el acceso a las oficinas, establecer medidas de organización que limiten el acceso a las personas concretas que requieran esa información (criterio "need-to-know") así como el uso de contraseñas y encriptaciones de la información electrónica.

En sentido similar, el Código Deontológico del Colegio de Abogados de Australia no recoge en la actualidad ninguna previsión expresa sobre las nuevas tecnologías, pero la revisión a dicho Código, de fecha 1 de febrero de 2018, plantea la necesidad de prestar atención a las nuevas prácticas de la profesión que utilizan como plataforma de intercambio de información la nube; en ellas, precisa el Informe, habrá que tener en cuenta quién es el proveedor de dicho servicio, especialmente si éste se encuentra fuera del país y queda sujeto a normas de confidencialidad diferentes a las australianas, asegurarse de que el cliente es consciente de las implicaciones del uso de dicha tecnología y si puede ser necesaria la encriptación[19].

Conclusión

A la vista de lo anterior, queda patente el notable atraso de la deontología europea en materia de seguridad digital, lo cual resulta preocupante si atendemos al creciente avance, sofisticación y expansión de los ataques cibernéticos, sobre los cuales trataremos en el siguiente apartado. Si aceptamos el axioma de que el Derecho debe acercarse lo máximo posible a la realidad social del momento, llama la atención el importante desfase existente entre la avanzada realidad tecnológica del momento y la

[19] "Review of the Australian Solicitors' Conduct Rules", Law Council of Australia, 2018, p. 43.

escasa y parca regulación que se recoge al respecto en los códigos deontológicos de la Unión Europea. En este sentido, convendría una actualización de las obligaciones éticas de la abogacía europea, de cara a reflejar las previsiones y cautelas que debemos adoptar en el ejercicio de la profesión para salvaguardar la información del cliente de las nuevas amenazas que hacen peligrar su integridad, disponibilidad y confidencialidad.

Riesgos cibernéticos a los que se enfrena la profesión y su impacto en la deontología

A la vista de la situación actual de la ciberseguridad en materia deontológica, resulta preciso en este momento pasar a analizar cuáles son los riesgos concretos a los que se enfrenta un abogado en su ejercicio diario, los cuales nos van a permitir averiguar si nuestro Código Deontológico ha quedado obsoleto y qué medios puede poner el Colegio de Abogados, los despachos y los propios abogados en su ámbito de actuación para prevenir y evitar posibles ataques cibernéticos.

A estos efectos, se analizará en primer lugar la naturaleza de los referidos riesgos cibernéticos para, acto seguido, estudiar su incidencia en los actuales deberes regulados en el Código Deontológico.

A) Principales riesgos cibernéticos que comprometen el ejercicio de la profesión

En este sentido, Francisco Pérez Bes, Secretario General del Instituto Nacional de Ciberseguridad ("INCIBE"), ha destacado tres grandes riesgos que afectan de modo especial al ejercicio de la abogacía: la suplantación de identidad, los ataques de denegación de servicio y las fugas de información[20].

[20] Pérez Bes, F., "La ciberseguridad en la deontología del abogado", *Abogacía Española*, 25 de mayo de 2017. Disponible en: http://www.abogacia.es/2017/05/25/la-ciberseguridad-en-la-deontologia-del-abogado/

1. Suplantación de identidad

En este caso, según Pérez Bes, *los atacantes crean, con propósitos ilícitos, perfiles falsos del despacho o de alguno/s de sus integrantes para robar información sensible de sus clientes, para perjudicar a su reputación, o para cometer fraudes online*[21].

Las principales técnicas que amenazan la identidad del despacho o sus abogados son el *phising* y el *pharming*.

Phising

El *phising* es un fraude patrimonial en el que *mediante comunicaciones electrónicas engañosas (correo electrónico), se consigue embaucar al perjudicado para que proporcione datos confidenciales (que posteriormente son utilizados para operaciones ilícitas normalmente en entidades financieras) que éste remite al autor del fraude, bien directamente o bien de forma mediata, esto es, pinchando en un link que le redirecciona a una página web fraudulenta que pertenece al citado aut*or[22].

Así, de acuerdo con nuestros tribunales, podemos distinguir cuatro fases típicas de esta modalidad de estafa informática[23]:

1) Obtención ilícita de credenciales bancarias, normalmente claves y contraseñas, mediante el envío masivo de correos haciéndose pasar por la entidad bancaria y pretendiendo cierta información confidencial del usuario.

2) Acceso a la cuenta bancaria de la víctima, cuya contraseña ha sido obtenida ilícitamente.

3) Realización de transferencias desde dicha cuenta a otra cuenta "mula" a la que se transfieren las cantidades fraudulentamente obtenidas. Dichas cuentas

[21] Pérez Bes, F., *op. cit.*

[22] Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, 2016.

[23] Sentencia núm. 256/2014 de la Audiencia Provincial de Albacete, de 9 de julio de 2014 (rec. 304/2014).

"mulas" están a nombre de terceros ("muleros"), los cuales reciben una comisión por participar en la operación.

4) Ingreso del dinero en la cuenta "mula" y posterior remisión por éste de dicho dinero a las personas autoras principales del delito.

En el ámbito de los despachos de abogados, este método se puede utilizar contra el propio despacho, sin perjuicio para clientes, o utilizando al despacho como medio para la obtención de información confidencial de los clientes.

En el primer caso, sirva de ejemplo el caso del despacho estadounidense Wallace & Wittman en 2013; en él, los criminales enviaron un correo electrónico al despacho, haciéndose pasar por un grupo industrial e informando de que una transferencia no había sido correctamente realizada. Dicho correo ofrecía un link para solucionar el problema, a través del cual los hackers instalaban un transcriptor de actividad en el ordenador desde el que se accedía al link y fueron capaces de rastrear las teclas pulsadas por el usuario y así poder conocer las contraseñas bancarias utilizadas por el despacho para, con dicha información, realizar una transferencia de $336.600 desde una cuenta del despacho a una cuenta en Moscú.

Otro ejemplo algo más reciente y cercano lo constituye la suplantación de identidad sufrida por Banco Santander durante este año, en la que clientes suyos (entre ellos, diversos despachos de abogados) recibieron correos de dicho banco por los que se informaba al usuario de que su cuenta bancaria había sido suspendida por motivos de seguridad, indicándole que accediese a un enlace para poder recuperar su cuenta. Dicho enlace redirigía al usuario a una página web que simulaba la del banco, aunque realmente se trataba de una página fraudulenta cuyo único objetivo era robar las credenciales de los usuarios que cayesen en la trampa.

En cuanto al segundo caso, cuando es el despacho el que es utilizado como medio por los hackers para acceder a información bancaria del cliente, cabe traer a colación la Sentencia núm. 615/2016 de la Audiencia Provincial de Barcelona, de 25 de julio de 2016 (rec. 23/2016), la cual ha establecido que la utilización de una cuenta de correo

electrónico ajena, sin autorización de su titular y suplantando su identidad, para ordenar al destinatario del correo (un cliente del despacho, por ejemplo) la realización de transferencias a favor del remitente del correo, cumple los presupuestos del *phising* y resulta constitutiva de un delito de estafa informática. Esta doctrina es plenamente aplicable al supuesto en que un despacho vea utilizado fraudulentamente su correo electrónico, permitiendo al ciberdelincuente comunicarse con clientes y obtener de ellos información confidencial.

Una vez producido el delito, cabe plantearse si la responsabilidad es del banco o del despacho de abogados. En este sentido, los tribunales han apreciado, como norma general, que salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave de la víctima del *phising*, la responsabilidad es del banco[24], lo cual no debe liberar a los despachos de abogados de la responsabilidad de establecer una política diligente en materia de ciberseguridad, pues de lo contrario podría considerarse que la omisión total por el despacho de cualquier tipo de medida de prevención conllevaría negligencia grave por su parte.

Pharming

Junto al *phising*, el *pharming* consiste en un *ataque informático a través del cual su autor manipula las direcciones DNS (Domain Name System) directamente en los servidores DNS o bien atacando un ordenador concreto, de tal forma que todos los usuarios que pretendieran acceder a esa dirección IP en el primer caso, o el usuario afectado en el segundo, se verían afectados por el fraude y serían conducidos a una página web falsa controlada por el autor, a través de la cual trata de recabar la información necesaria para obtener el beneficio económico*.[25]

La técnica del *pharming* ha sido abordada por numerosos tribunales de nuestro país, pudiendo traer a colación, por su claridad expositiva, la explicación ofrecida por la

[24] Sentencia núm. 190/2015 de la Audiencia Provincial de Madrid, de 4 de mayo de 2015 (rec. 6/2014).

[25] VV.AA., *Memento Práctico. Derecho de las Nuevas Tecnologías 2017-2018*, Francis Lefebvre, 2017, p. 485.

Audiencia Provincial de Valencia en sus Sentencias de 28 de enero de 2016 (rec. 242/2015) y 5 de septiembre de 2016 (rec. 989/2016):

> *También hay que tener en cuenta el pharming, sistema por el cual los ciber delincuentes hacen cambios en un ordenador de manera que cuando se accede los servicios bancarios por internet no se ve la página original del Banco con el que se quiere operar legítimamente, sino otra que la imita a la perfección. Cuando el usuario introduce sus datos en estas páginas, los mismos van a parar directamente a los defraudadores que los utilizan después de forma ilícita disponiendo traspasos desde la cuenta del perjudicado*.

La diferencia fundamental entre el *phising* y el *pharming* radica en la necesidad de una actuación previa por parte de la víctima para la efectividad del fraude. Así, mientras el *phising* suele requerir que el usuario acceda al link engañoso enviado por el delincuente, el *pharming* modifica las DNS, sin conocimiento del usuario, de modo que cuando éste último intente acceder a una página de su confianza (la página de su banco, por ejemplo), será redirigido a una página falsa prácticamente idéntica a la pretendida, pero con una dirección IP diferente, a través de la cual el autor del fraude tratará de obtener información confidencial de la víctima.

Por tanto, el *pharming* es un tipo de estafa que va un paso por delante del *phising*, toda vez que, modificando las DNS, cualquier usuario que pretenda acceder a un determinado dominio será reconducido a otro visualmente idéntico pero de distinta IP, manipulado por el delincuente al objeto de su lucro personal. De este modo, el *pharming* crea un grupo de usuarios vulnerables mucho mayor que el *phising*.

De acuerdo con el magistrado Eloy Velasco, tanto el *phising* como el *pharming* son un *tipo delictivo complejo*, integrados por diversas fases, cada una constitutiva de un tipo penal. En síntesis, los referidos fraudes informáticos se caracterizan por:

1) Una inicial suplantación de identidad, constitutiva de un delito de *falsedad en documento mercantil* (artículo 392 del Código Penal).

2) Una fuga de datos, constitutiva de un delito de *descubrimiento de datos informáticos secretos* (artículo 197.2 del Código Penal).

3) Un robo de dinero, constitutivo de una *estafa informática* (artículo 248 del Código Penal).

Asimismo, en caso de no llegar a producirse el apoderamiento patrimonial final, debe mantenerse una consideración del fraude en su conjunto, de modo que la realización imperfecta del mismo debe penarse como tentativa[26].

2. Ataques de denegación de servicio

Un ataque de denegación de servicio consiste en *dejar un sistema informático fuera de servicio haciendo que no puedan atender peticiones de usuarios legítimos*[27]. Estos ataques pueden consistir en el envío de millones de peticiones al servidor con el objetivo de ralentizarlo, en la saturación de un servidor con grandes paquetes de información o en el envío de peticiones desde una dirección IP falsa[28].

Para llevar a cabo dichos ataques masivos, los cibercriminales se sirven de redes "botnet", conjunto de computadoras controladas de manera remota por el delincuente[29], a partir de las cuales puede realizar este tipo de actuaciones en masa.

Si bien este tipo de ataques se suelen dirigir contra grandes servidores de la web[30], nada impide que los despachos de abogados se puedan ver afectados[31], por lo que deviene fundamental tomar las medidas necesarias para evitar este tipo de ataques.

---

[26] Velasco Núñez, E., "Fraudes informáticos en red: del *phising* al *pharming*", *La Ley Penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, nº 37, 2007, pp. 57-66.

[27] Sentencia de la Audiencia Provincial de Tarragona, de 23 de julio de 2001 (rec. 735/2000).

[28] VV.AA., "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", *Systems, cybernetics and informatics*, volume 3, número 1, 2014, p. 66.

[29] Para alcanzar dicho control, el cibercriminal habrá usado previamente virus troyanos especiales para vulnerar la seguridad de las computadoras de varios usuarios, obteniendo el control conjunto de todas ellas para conformar una red "botnet".

[30] Un ejemplo de ello fue el ataque sufrido por Yahoo, eBay, Amazon, CNN y otros grandes sitios web los días 6 y 7 de febrero de 2000, en la que sus portales de internet se apagaron temporalmente a causa del ataque de denegación de servicio orquestado por Michael Calce.

De hecho, en lo que a España concierne, el mundo de la abogacía se vio recientemente afectado por el ataque de denegación de servicio orquestado contra LexNet, el sistema de notificaciones judiciales que utilizan los juzgados, procuradores y abogados españoles. Este ataque, perpetrado en septiembre de 2017, consistió en el envío masivo de peticiones simultáneas con el objetivo de colapsar y hacer inaccesible LexNet a los usuarios legítimos del mismo.

Asimismo, dado su alcance y peligrosidad, conviene señalar que la Fiscalía General del Estado, en su Circular núm. 3/2017, de 21 de septiembre, ha ubicado expresamente los ataques de denegación de servicio en el tipo del artículo 264 bis.1.b) del Código Penal, cuyo tenor establece (énfasis añadido):

> *1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:*
>
> *a) realizando alguna de las conductas a que se refiere el artículo anterior;*
>
> *b) introduciendo o transmitiendo datos; o*
>
> *c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.*
>
> *(...).*

A la vista de la magnitud de los daños que se pueden irrogar tanto al titular del dominio web afectado como al cliente que se ve impedido de acceder a dicho servicio, podemos anticipar la importancia que tendrá la ciberseguridad como deber deontológico del abogado para garantizar el acceso de sus clientes a la página web del despacho.

[31] Así ocurrió con los despachos estadounidenses Cravath, Swaine & Moore LLP y Weil Gotshal & Manges LLP en 2016.

3. Fugas de información

De acuerdo con el INCIBE, la fuga de información es la *liberación deliberada o involuntaria de información confidencial o sensible, a un medio o a personas que no deberían conocerla*[32].

A diferencia de los anteriores riesgos cibernéticos, que pueden afectar en casos excepcionales a los despachos de abogados, la fuga de información constituye una amenaza constante en el ejercicio diario de la profesión. Téngase en cuenta la información sensible de empresas y personas físicas de que disponen los abogados con ocasión del ejercicio de su profesión y la utilidad y valor que ésta puede reportar a terceros interesados. Cómo dato significativo de la recurrencia de este riesgo, un estudio llevado a cabo sobre la ciberseguridad en más de 200 despachos de abogados estadounidenses, acreditó que un 66% de la muestra había sufrido algún tipo de fuga de información durante el año 2016, de los que aproximadamente un 40% no sabía que había sufrido dicha fuga[33].

Entre las causas que producen la fuga de información en un despacho de abogados, el INCIBE ha diferenciado entre causas organizativas y técnicas[34]:

a) Causas organizativas: falta de clasificación de la información en base a su nivel de confidencialidad, falta de delimitación del ámbito de difusión de la información, falta de conocimiento y formación, ausencia de procedimientos y obligaciones para los abogados en el ámbito de ciberseguridad o inexistencia de acuerdos de confidencialidad.

b) Causas técnicas: código malicioso o malware, acceso no autorizado a sistemas e infraestructuras, generalización del uso de servicios en la nube o uso de las tecnologías móviles para el trabajo diario.

---

[32] INCIBE, "¿Estás preparado para hacer frente a una fuga de datos?", *Blog*, 2017. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

[33] Logicforce, "Law Firm Cyber Security Scorecard", 2017, p. 6.

[34] Abogacía Española, "Cómo gestionar una fuga de información en un despacho de abogados", *Guías TIC*, 2016, pp. 11-14.

Como ejemplo paradigmático de fuga de información en un despacho de abogados, podemos traer a colación el mediático caso del despacho Mossack Fonseca (*Papeles de Panamá*), cuyos servidores fueron atacados para la obtención de cientos de correos electrónicos, cuentas bancarias, bases de datos, pasaportes y registros de clientes. Algunos medios de comunicación atribuyen como factores de riesgo que pudieron propiciar esta fuga el hecho de que el despacho utilizaba un único servidor, tenía el *plugin* desactualizado y no había cambiado en tres años las contraseñas de acceso[35]; según la anterior clasificación elaborada por el INCIBE, estas causas serían de tipo organizativo, en contraposición al supuesto ataque externo que desató la fuga de información, que sería de tipo técnico.

A la vista de lo anterior, la ciberseguridad deberá ser un elemento indispensable en la estrategia de los despachos de abogados, así como en la esfera individual de cada abogado, incorporándola a su haz de deberes deontológicos.

B) Incidencia en la deontología del abogado

Una vez detallados los anteriores riesgos cibernéticos, los cuales pueden incidir en la esfera de cualquier profesión mínimamente afectada por la digitalización, llega el momento de analizar su impacto concreto en la deontología del abogado, como tema esencial de este trabajo.

Aunque pueda parecer, en una primera aproximación, que ciberseguridad y deontología son compartimentos estancos en el ejercicio de la abogacía, conviene recordar las palabras de Carlo Lago, al afirmar que *todo comportamiento del profesional que no tenga un carácter meramente técnico, pero que esté vinculado de cualquier forma al ejercicio de la profesión, entra en el ámbito de la normativa deontológica*[36]. En este sentido, resulta evidente que el ejercicio de la abogacía, hoy en día, se ve envuelto en un entorno digital que impide desconocer las más elementales medidas de seguridad tendentes a garantizar la protección y confidencialidad de la valiosa información que

[35] Ver noticia completa en: https://www.elconfidencialdigital.com/dinero/filtracion-Mossack-Fonseca-errores-informaticos_0_2690130975.html

[36] Lega, C., *Deontología de la profesión de abogado*, Civitas, Madrid, 1983, p. 25.

obra en poder de los despachos de abogados. Consecuencia inmediata de lo anterior, y siguiendo la cita de Carlo Lago, es la debida observancia que la deontología de la profesión debe prestar a dicho escenario digital.

En la medida que el Código Deontológico de la profesión carece de la deseable mención a la ciberseguridad como deber deontológico, el presente análisis se verá circunscrito a una serie de deberes que, al momento de su redacción, no fueron concebidos para garantizar la seguridad de la información en soporte digital a disposición del abogado (un ejemplo ilustrativo de que, por lo general, la realidad antecede al Derecho). A estos efectos, se exponen a continuación los deberes deontológicos que, a mi juicio, se pueden ver más afectados por los nuevos riesgos cibernéticos que acechan el ejercicio de la profesión:

i. Deber de independencia

Inserto en el artículo 2 del Código Deontológico, este deber se articula como auténtico eje vertebrador del ejercicio de la profesión, garantizando el efectivo derecho de defensa de los ciudadanos. Así, de acuerdo con el artículo 2.2 del Código Deontológico:

> *Para poder asesorar y defender adecuadamente los legítimos intereses de sus clientes, el abogado tiene el derecho y el deber de preservar su independencia frente a toda clase de injerencias y frente a los intereses propios o ajeno*s.

A este respecto, si bien la mayor parte de los ataques informáticos detallados a lo largo del presente trabajo se han tratado desde la voluntad aséptica del delincuente que únicamente persigue obtener un lucro económico con el ciberataque, sin pretender generar en el despacho de abogados un perjuicio adicional al meramente económico, existen otros casos en los que el delincuente, sin buscar necesariamente un lucro económico, busca perjudicar la imagen y reputación del despacho por razón del tipo de clientes o causas que defiende (práctica conocida en el argot anglosajón como *hacktivism*).

Este tipo de ataques intencionados y dirigidos hacia un despacho en concreto pueden llegar a poner en serio peligro la independencia de sus abogados, dado que se verán

coaccionados para dejar de defender a ciertos clientes o causas, sin poder llevar a cabo su ejercicio profesional con plena libertad.

A título ejemplificativo, estos ataques a la reputación e imagen del despacho se han materializado en la publicación indebida de información confidencial[37] o en ataques de denegación de servicio[38]. En ambos casos, el perjuicio generado excede intencionadamente el ámbito de lo meramente interno, dañando la imagen pública del despacho, con el fin de denunciar ciertas causas que esté defendiendo el mismo.

En otras ocasiones, en cambio, el delincuente no busca directamente dañar la imagen pública del despacho, sino acceder a sus servidores con el fin de desvirtuar de cualquier modo la defensa que esté llevando de cualquier cliente. Por ejemplo, podemos traer a colación el caso del despacho estadounidense Gipson, Hoffman & Pancione, que en 2010 sufrió ataques de *phising* por parte de hackers chinos tras demandar a la República Popular China, en nombre de CYBERsitter, por piratería.

Evidentemente, estos ataques chocan frontalmente con las más elementales exigencias del deber de independencia, lo que exige del abogado la incorporación de la ciberseguridad a su haz de deberes deontológicos, pues, en última instancia, la debida independencia del abogado redundará en una mejor defensa de los intereses del cliente.

Si bien esta obligación de velar por la debida protección de los sistemas informáticos del despacho la podríamos incardinar en el genérico tenor del artículo 2 del Código Deontológico, se echa en falta una regulación más específica y detallada del alcance de la ciberseguridad como deber deontológico, pues ello permitirá delimitar con mayor precisión los casos en los que el abogado incurrirá en responsabilidad disciplinaria de

---

[37] Un caso paradigmático de este tipo de ataques fue el sufrido por el despacho estadounidense Puckett & Faraj en 2012, que, defendiendo a un sargento estadounidense culpable de la muerte de 24 civiles desarmados en Haditha (Irak) fue objeto de un ciberataque que resultó en la publicación de cientos de correos del despacho sobre el caso. Presuntamente, el objetivo perseguido por los delincuentes era de naturaleza política, buscando el fin de la presencia militar de Estados Unidos en Irak.

[38] En relación con los ataques de denegación de servicio, el Consejo General de la Abogacía Española ha reconocido que "Este tipo de ataques están cobrando cada vez más relevancia pública como forma de ciberprotesta (*ciberhacktivismo* en el argot), que puede provenir de algún caso o asunto en el que el despacho pueda estar involucrado". Abogacía Española, "Guía de Ciberseguridad y Reputación Online para Despachos de Abogados", *Guías TIC*, 2012, p. 16.

aquellos en los que, por haber tomado todas las medidas exigibles, su actuación debe entenderse acorde con la diligencia debida.

ii. Deber de confianza e integridad

Por su parte, el deber de confianza e integridad nos recuerda que nuestra labor no es un mero ejercicio abstracto de interpretación del Derecho, sino que es fruto del compromiso previo con un cliente que ha depositado su confianza en nosotros para ofrecerle una adecuada defensa de sus intereses. En consecuencia, es un deber del abogado corresponder esa confianza con el despliegue de la máxima diligencia en su ejercicio profesional. En este sentido, de acuerdo con el artículo 4.1 del Código Deontológico:

> *La relación entre el cliente y su abogado se fundamenta en la confianza y exige de éste una conducta profesional íntegra, que sea honrada, leal, veraz y diligente.*

Este deber adquiere especial relevancia en el contexto del presente trabajo, pues el cliente confía en que el despacho de abogados adopte las medidas tendentes a la correcta protección y salvaguarda de la información que aquel le confíe a éste para un adecuado servicio jurídico, de modo que todo ataque cibernético que sufra el despacho de abogados perjudicará la confianza que el cliente ha depositado en él.

A la vista de lo anterior, dada la alta probabilidad de que se vulnere ese deber de confianza e integridad al más mínimo ataque informático que sufra el despacho, resulta patente la necesidad de incorporar al ejercicio profesional una serie de técnicas preventivas de orden informático que aseguren la información a disposición del despacho y salvaguarden la confianza depositada por el cliente.

Llegados a este punto, conviene recordar las modificaciones realizadas por la American Bar Association en su *Resolution 105A, Commission on Ethics 20/20*, a las que hicimos referencia con motivo del estudio de la regulación deontológica en otras jurisdicciones. Entre dichas modificaciones, resulta de especial interés, a los efectos del deber de confianza e integridad, la inclusión del conocimiento de los riesgos derivados de las

nuevas tecnologías como parte del debido conocimiento técnico que debe poseer el abogado. Así, establecía la citada Resolución la siguiente previsión:

> *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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject*.[39]

En línea con lo anterior, echamos en falta en la presente regulación del Código Deontológico algún precepto que desarrolle el concepto de actuación diligente[40] al que alude el citado artículo 4, en el sentido de incorporar alguna previsión como la anteriormente transcrita que prevea el necesario conocimiento de las nuevas tecnologías, y los riesgos asociados a las mismas, como condición necesaria para la calificación de una actuación como diligente.

En el mundo digitalizado de hoy en día, el cliente de un despacho de abogados esperará que éste adopte las medidas necesarias para evitar cualquier tipo de ataque informático, por lo que la diligencia que se le exigirá al abogado deberá incorporar una serie de actuaciones tendentes a la protección de sus sistemas informáticos para salvaguardar, en última instancia, la información relacionada con sus clientes.

iii. Deber de secreto profesional

Junto a los anteriores, otro de los deberes deontológicos que se ve claramente afectado por el nuevo escenario digital es el deber de secreto profesional, de importancia capital

[39] Resolution 105A, Commission on Ethics 20/20, *op. cit.* p. 3.

[40] Los órganos jurisdiccionales no han tenido ocasión de pronunciarse aún sobre el alcance de la diligencia del abogado en relación con las nuevas tecnologías, por lo que solamente podemos acudir a la clásica y vaga previsión establecida por el Tribunal Supremo sobre el deber de diligencia del abogado en abstracto, estableciendo que su "exigencia debe ser mayor que la propia de un padre de familia dados los cánones profesionales recogidos en su Estatuto" (Sentencias del Tribunal Supremo de 4 de febrero de 1992 [rec. 2618/1989) y 14 de mayo de 1999 [rec. 3590/1994])

en el ejercicio de la profesión[41], el cual queda definido en el artículo 5.1 del Código Deontológico en los siguientes términos:

> *La confianza y confidencialidad en las relaciones entre cliente y abogado, ínsita en el derecho de aquél a su intimidad y a no declarar en su contra, así como en derechos fundamentales de terceros, 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 cualquiera de las modalidades de su actuación profesional, sin que pueda ser obligado a declarar sobre los mismos como reconoce el artículo 437.2 de la vigente Ley Orgánica del Poder Judicial.*

El deber de secreto profesional ha experimentado un antes y un después con la era digital, puesto que, si bien antes, el quebrantamiento del derecho se solía producir por una conducta activa del abogado, en la actualidad, también se puede producir por una conducta pasiva del abogado que no protege adecuadamente sus sistemas, abriendo la vía al acceso no autorizado de terceras personas.

El supuesto paradigmático que pone en tela de juicio la integridad del secreto profesional es la fuga de información. A este respecto son numerosos los casos de despachos de abogados que han sufrido fugas de información provocadas por delincuentes que, en la mayoría de las ocasiones, persiguen dañar la imagen pública del despacho o la de sus clientes[42].

Si atendemos al tenor del artículo 5.1 del Código Deontológico, observamos cómo el deber de secreto profesional se establece en términos absolutos, de modo que toda filtración que se produzca sobre información concerniente a clientes implicaría el desacato del secreto profesional.

---

[41] Tanto es así que Juan José Torres-Fernández Nieto ha llegado a aseverar que *no puede existir abogacía libre e independiente sin secreto profesional*. Torres-Fernández Nieto, J.J., *Deontología Profesional de la Abogacía*, Siglo XXI Legal, Madrid, 2018, p. 87.

[42] En este sentido, podemos traer a colación los casos de los despachos de abogados Mossack Fonseca y Appleby, ambos residentes en paraísos fiscales (Panamá e Islas Bermudas, respectivamente), los cuales fueron objeto de fugas de información cuyo objeto era sacar a la luz pública el nombre de los personajes públicos que operaban con sociedades *offshore* y que podían estar ocultando dinero a la Hacienda Pública de sus países.

En mi opinión, esta redacción se encuentra desactualizada, pues atiende a un momento temporal en el que el incumplimiento del secreto profesional sólo se producía por una conducta activa del abogado que filtraba cierta información de clientes a terceros. En estos casos, evidentemente, cualquier filtración que se produjese era inexcusable, pues provenía de una actuación negligente y dolosa del abogado.

En la actualidad, en cambio, se pueden producir fugas de información aún en el caso de haber adoptado todas las medidas de prevención razonables y exigibles, pues los nuevos medios de almacenamiento de la información dependen de un sistema virtual que escapa del completo control por parte del abogado.

De nuevo, conviene traer a colación la reforma realizada por la American Bar Association en su *Resolution 105A, Commission on Ethics 20/20*, la cual establecía, en relación con la debida confidencialidad de la información, la siguiente previsión:

> *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*.[43]

A la vista de la indeterminación que implicaría determinar el alcance de la razonabilidad referida por el precepto, la propia Resolución establece como factores a tener en cuenta para determinar *ad casum* la razonabilidad de los esfuerzos empleados: la importancia de la información, la probabilidad de revelación de dicha información si no se adoptan otras medidas, el coste de implementar esas medidas adicionales de seguridad, la dificultad de dicha implementación y el grado en que dichas medidas puedan perjudicar la habilidad del abogado para representar a su cliente

Al igual que sucedía en sede del deber de confianza e integridad, donde se expuso el deseable desarrollo del alcance de la diligencia debida, el deber del secreto profesional plantea un problema similar, al dejar al albur del Juez la delimitación de aquellos casos en los que el ataque informático es consecuencia de la negligencia del abogado de

[43] Resolution 105A, Commission on Ethics 20/20, *op. cit.* p. 4.

aquellos otros en los que nada se pudo achacar a la labor de prevención y protección empleada por el letrado.

En base a lo expuesto, sería recomendable incorporar al Código Deontológico una serie de pautas, en línea con las ofrecidas por la citada Resolución de la American Bar Association, que ayuden al órgano juzgador a llevar a cabo dicha delimitación y doten de seguridad jurídica a los despachos en relación con las prevenciones establecidas en materia de ciberseguridad.

Propuestas y soluciones

Tomando en consideración todos los aspectos detallados a lo largo del presente trabajo, estamos en condiciones de plantear diversas propuestas de mejora de cara a integrar el ejercicio profesional de la abogacía con las nuevas vicisitudes que derivan del nuevo escenario tecnológico. En este sentido, dividiré la exposición de las diversas propuestas y soluciones en aquellas que sean de tipo regulatorio y aquellas otras que deban implementarse en la esfera personal de cada abogado o en el ámbito interno de un despacho.

Aspectos a considerar en el ámbito regulatorio

En lo concerniente a la regulación, aflora como prioridad la necesaria modificación del Código Deontológico a los efectos de incluir la ciberseguridad como deber deontológico del abogado. Esta necesidad ya quedó patente al comparar la regulación actual de los códigos deontológicos de los países de la Unión Europea con aquella de los países anglosajones. En este sentido, sería conveniente una actualización del Código de Deontología de los Abogados Europeos, con la consecuente modificación del Código Deontológico de la Abogacía Española.

Así, a pesar de que, con ocasión del análisis de los deberes deontológicos afectados por las nuevas tecnologías, se han ido desengranando las carencias regulatorias de los deberes de independencia, confianza e integridad y secreto profesional, considero que sería preferible dedicar un artículo específico a la ciberseguridad, en vez de añadir pequeñas matizaciones al hilo del desarrollo de cada deber deontológico. De este modo,

se lograría un desarrollo unificado de la ciberseguridad como deber deontológico, el cual se proyectaría e incidiría sobre el resto de deberes deontológicos.

A estos efectos, considero que el citado artículo debería abordar los siguientes aspectos:

1. **Debido conocimiento de los riesgos asociados a las nuevas tecnologías**

Si bien esta obligación se insertaría en lo que en otras jurisdicciones se denomina la necesaria competencia profesional[44], en el Código Deontológico español cabe entender subsumida dicha competencia en el deber de confianza e integridad que el abogado debe mantener frente a su cliente, concretamente, en la conducta diligente que debe emplear el abogado. Asimismo, el artículo 13.8 del Código Deontológico establece que *[e]l Abogado no aceptará ningún asunto si no se considera o no debiera considerarse competente para dirigirlo, a menos que colabore con un Abogado que lo sea*.

Con esta previsión expresa, se lograría una mayor concienciación formativa, la cual se podría fomentar mediante la inclusión de contenidos sobre ciberseguridad en las pruebas de acceso a la profesión, en la implementación de cursos formativos *online* o presenciales por los despachos de abogados[45] (o por el Colegio de Abogados de cada circunscripción) o en la promoción de congresos y conferencias sobre la materia.

2. **Obligación de implementar todas las medidas razonables para la correcta protección de la información de clientes frente a terceros**

Esta obligación podría considerarse ínsita en el deber de secreto profesional, si bien por su entidad e importancia considero que debería ser objeto de regulación aparte en un precepto dedicado a la ciberseguridad, en el cual podría obtener el desarrollo deseable.

---

[44] Podemos encontrar previsiones expresas sobre el deber deontológico a la competencia profesional en los Códigos Deontológicos de Estados Unidos, Canadá, Japón y Nueva Zelanda, entre otros. A efectos aclaratorios sobre la naturaleza de este tipo de previsiones, podemos traer a colación la regulación prevista en el *Lawyers and Conveyancers Act Rules 2008* de Nueva Zelanda, en cuyo artículo 3.9 se establece: "A lawyer must undertake the continuing education and professional development necessary to ensure an adequate level of knowledge and competence in his or her fields of practice."

[45] En este sentido, son varios los despachos de abogados que ya han incorporado cursos *online* sobre ciberseguridad de obligada realización para sus abogados, lo que denota que la práctica profesional se está anticipando a la regulación normativa.

En dicho desarrollo se debería precisar el alcance de esa razonabilidad que exima al abogado de responsabilidad disciplinaria. A estos efectos, puede resultar interesante la adopción de un sistema de *compliance* similar al establecido en el artículo 31.bis del Código Penal para la exención de responsabilidad penal de las personas jurídicas[46]. En este caso, la adopción por el abogado de una serie de medidas preventivas de orden tecnológico le eximiría de responsabilidad disciplinaria.

En este sentido, el Consejo General de la Abogacía Española ha previsto en su Plan Estratégico para 2020 un programa de ciberseguridad para Colegios, despachos y comunicaciones entre abogados que podría ir en la línea del sistema de *compliance* del orden penal. Así, esboza las líneas de dicho programa en los siguientes términos:

> *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 (...).*[47]

Por su parte, si bien en sede de responsabilidad civil, este mismo modelo de *compliance* se podría adoptar por las aseguradoras en sus pólizas de seguros, a fin de reducir el riesgo de que los despachos de abogados sean víctimas de un ataque informático

Una vez expuestas las recomendaciones regulatorias que deberían llevar a la inclusión de la ciberseguridad en el Código Deontológico de la Abogacía, cabe recordar que dicha inclusión no sería una mera declaración de intenciones, ni mucho menos un brindis al sol, sino que el incumplimiento de las obligaciones asociadas a la ciberseguridad sería constitutivo de responsabilidad disciplinaria. Así lo ha declarado reiteradamente el Tribunal Constitucional en los siguientes términos:

---

[46] Este sistema de *compliance* ha recibido el beneplácito del Tribunal Supremo, al establecer en su reciente Sentencia de 28 de junio de 2018 (rec. 2036/2017) que "una buena praxis corporativa en la empresa es la de implementar estos programas de cumplimiento normativo que garanticen que este tipo de hechos no se cometan, o dificulten las acciones continuadas de distracción de dinero, o abusos de funciones que un buen programa de cumplimiento normativo hubiera detectado de inmediato."

[47] Consejo General de la Abogacía Española, "Plan Estratégico Abogacía 2020", 2017, p. 42.

> *(...) 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 y responden a las potestades públicas que la Ley delega en favor de los Colegios (...).*[48]

En virtud de lo expuesto, la inclusión de la ciberseguridad como deber deontológico resultaría en la incorporación por todos los despachos de abogados de las necesarias medidas preventivas de orden tecnológico, en la consecuente reducción de la tasa de éxito de los ataques cibernéticos y, en última instancia, en la protección de la información del cliente y en la mejora del servicio de defensa prestado a éste.

Aspectos a incorporar en la práctica profesional

Por último, y sin ánimo de realizar una enumeración exhaustiva de todas las medidas posibles, a continuación expondré una serie de medidas que, a mi juicio, pueden resultar de particular interés para su implementación en la esfera individual de cada abogado.

1. **Utilización de una nube privada**

En caso de que el despacho de abogados tenga contratados ciertos servicios en la nube, resulta altamente recomendable que estos utilicen un modelo de despliegue en nube privada, en contraposición a la nube pública o híbrida.

Cuando los servicios se prestan desde una nube privada, *los recursos se entregan de forma exclusiva, privada, al despacho de abogados, al que se le ofrece el control sobre el servicio que alquila*[49]. Este sistema reporta grandes ventajas en términos de seguridad y privacidad de los datos y procesos, si bien resulta más costoso que la utilización de una nube pública. De todos modos, dada la sensibilidad y confidencialidad de la

[48] Sentencias del Tribunal Constitucional de 21 de diciembre de 1989 (rec. 1440/1987) y 5 de diciembre de 2013 (rec. 8434/2006).

[49] Abogacía Española, "Cloud computing. Una guía de aproximación para la abogacía", *Guías TIC*, 2012, p. 19.

información tratada por un despacho de abogados, la seguridad y protección de los datos almacenados debería primar sobre el coste de su aseguramiento.

Asimismo, la contratación de un servicio en nube privada permite la posibilidad de negociar los Acuerdos de Nivel de Servicio, los cuales regulan los compromisos adquiridos entre el proveedor del servicio y el cliente durante la prestación de dicho servicio[50]. Esta posibilidad no existiría en el caso de una nube pública, donde las cláusulas del contrato suelen ser innegociables.

2. Encriptación y tokenización

De todas las medidas concretas que se podrían adoptar, interesa destacar la encriptación y tokenización, por su efectividad y seguridad frente a injerencias externas, así como por su relación con la utilización de servicios en la nube.

La encriptación consiste en la codificación de la información, haciéndola inaccesible a terceros usuarios. Esta codificación garantiza que sólo puedan visualizar la información el emisor y receptor de la misma, mediante una clave que el primero habrá suministrado al segundo a tal efecto.

Por su parte, la tokenización es el proceso por el cual se sustituye información sensible por un conjunto de símbolos (conocido como *token*) que retienen toda la información esencial sin comprometer su seguridad y que, en caso de sustracción, carecen de valor alguno para el ciberdelincuente. Su mayor aplicación radica en la salvaguarda de los datos bancarios con ocasión de las transferencias realizadas, sustituyendo los números de cuenta o tarjeta de crédito por un *token* que carece de valor alguno para cualquier tercero que pretenda sustraer dicha información.

---

[50] A este respecto, el informe "Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal" ha detallado una serie de aspectos a tener en cuenta por los despachos a la hora de negociar estos acuerdos. Entre ellos, destaca el compromiso del proveedor de disponer de los mecanismos necesarios de recuperación de la información, de la copia de seguridad necesaria para garantizar la integridad y conservación de la información y de garantizar que la información sólo será accesible para el despacho de abogados. Abogacía Española, "Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal", 2012, pp. 16-17.

En el ámbito de un despacho de abogados, la encriptación puede ser altamente efectiva para la protección de cierta documentación sensible que pueda recibirse del cliente (e.g. información bancaria, personal o patrimonial, así como la relativa a proyectos empresariales); asimismo, su utilidad se puede extender a los procesos de *due diligence*, protegiendo la información de las sociedades involucradas en la operación a la que puedan tener acceso sus respectivos abogados con motivo del *Q&A*.

Por su parte, la tokenización, de gran utilidad en los medios de pago, puede reportar grandes ventajas en todas las transferencias que atañen a un despacho de abogados, como las provisiones de fondos que realice un cliente al abogado, los pagos realizados por el despacho por gastos a cuenta del cliente, etc.

3. Código de conducta interno

Como alternativa, o complemento, a la regulación deontológica, no es descartable la posibilidad de elaborar un código de conducta interno que aborde los distintos protocolos y actuaciones que deban adoptar los abogados de un despacho en materia de ciberseguridad[51].

Esta posibilidad permitiría al despacho adaptar su política de ciberseguridad a las necesidades y exigencias concretas que se deriven del perfil de sus clientes y del tipo de información que éstos le confíen al despacho.

No obstante, el INCIBE ha elaborado una serie de políticas de cara a que puedan ser voluntariamente implementadas por cada empresa, por lo que, a falta de un código de conducta propio, sería aconsejable el compromiso del despacho de abogados con dichas políticas. En este sentido, el referido Instituto ha señalado que *[l]a normativa interna va a plasmar la forma en la que abordamos la ciberseguridad, es decir, nuestros compromisos. (…) El empresario tiene que informar al empleado de los usos aceptables*

[51] Esta opción fue planteada por Aldo Olcese y Tomás González Cueto en la Conferencia celebrada el día 18 de julio de 2017 bajo el título "La ciberseguridad en la abogacía como elemento de la confianza digital: buenas prácticas y RSE", organizada por el Consejo General de la Abogacía Española.

y no aceptables, por ejemplo con estas políticas, normativas y buenas prácticas: (...).[52] A tal efecto, el INCIBE ha elaborado, entre otras, una política de uso de dispositivos personales, una política de uso de portátiles, una clasificación de la información corporativa y una política de contraseñas.

4. Seguro de responsabilidad civil

Si bien el sistema de *compliance* que planteábamos para la regulación deontológica de la ciberseguridad podría llegar a eximir al abogado de responsabilidad disciplinaria, ello no le eximiría de la correspondiente responsabilidad civil.

Por ello, puede ser aconsejable la contratación de un seguro de responsabilidad civil que proteja al abogado de las repercusiones económicas que la responsabilidad civil derivada de cualquier ciberataque pudiera acarrear[53].

No obstante, la contratación de este tipo de seguros no debería ser un sustituto del adecuado sistema de protección y prevención que todo despacho debería implementar. En este sentido, el seguro de responsabilidad civil frente a ciberataques se constituiría como una medida más, en este caso con carácter *ex post*, para la reducción de los costes asociados a un ataque informático.

5. Machine learning

Por último, no quisiera concluir este apartado sin hacer una breve pero importantísima referencia a los nuevos avances que se están dando en el ámbito del *machine learning*. Esta tecnología permitiría que desarrollos algorítmicos pudieran detectar por sí mismos los problemas que afectasen a la integridad de un sistema informático y los corrigiesen en tiempo real.

Si bien aún es pronto para ver implantada este tipo de tecnología en la actualidad, habrá que prestarle especial atención para sopesar su incorporación en un futuro cercano.

---

[52] INCIBE, "Decálogo ciberseguridad empresas. Una guía de aproximación para el empresario", 2017, p. 5.

[53] Kroll, K.M., "Cyber Coverage: Separate policy, certain provisions needed for data protection", *ABA Journal*, 2016.

Conclusión

Afirmaba el profesor Enrique Dans que *[l]a ciberseguridad, en este momento, responde a muy pocos axiomas o verdades absolutas. Pero hay una que se hace cada día más evidente: si existe un interés muy elevado en acceder a un sistema determinado, se logrará, de una manera u otra acceder a él independientemente de la calidad de los profesionales que traten de impedirlo*[54].

En consecuencia, no debemos tomar la ciberseguridad como la panacea que protegerá definitivamente a los sistemas de un despacho de abogados de cualquier injerencia externa que pretenda un acceso desautorizado a información confidencial del despacho; siempre existirá el riesgo de que un ataque cibernético alcance sus objetivos. Ahora bien, la proporción de ataques exitosos debería ser absolutamente excepcional si se toma el firme compromiso de implantar la ciberseguridad como política esencial del despacho, a lo cual coadyuvaría notablemente la incorporación de ésta como deber deontológico del abogado.

Esta inclusión de la ciberseguridad en el haz de deberes deontológicos no solo serviría para actualizar el Código Deontológico, sino que supondría un paso hacia delante de la Abogacía en lo referente al nuevo cambio tecnológico, una apuesta innovadora y acertada que acercaría esta alta profesión a las nuevas vicisitudes del entorno digital.

De acuerdo con Adolfo Menéndez, *el futuro es de los que piensan más, antes y mejor*[55], sirva pues esta máxima como una invitación al sector de la abogacía para acompasar su código deontológico a los nuevos cambios tecnológicos que están afectando a la profesión.

---

[54] Dans, E., "Ciberseguridad: mucho que replantear", *HP Business Blog* ,15 de julio de 2016. Disponible en: https://blog.ext.hp.com/t5/BusinessBlog-es/Ciberseguridad-mucho-que-replantear/ba-p/6922

[55] Entrevista concedida por Adolfo Menéndez a la revista ONE, 17 de agosto de 2014.

BIBLIOGRAFÍA

❖ Obras monográficas

Delgado Martín, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley, 2016.

Lega, C., *Deontología de la profesión de abogado*, Civitas, Madrid, 1983.

Ossorio y Gallardo, A., *El alma de la toga*, Reus, Madrid, 2008.

Torres-Fernández Nieto, J.J., *Deontología Profesional de la Abogacía*, Siglo XXI Legal, Madrid, 2018.

VV.AA., *Memento Práctico. Derecho de las Nuevas Tecnologías 2017-2018*, Francis Lefebvre, 2017.

VV.AA., *The Privacy, Data Protection and Cybersecurity Law Review*, Law Business Research, 2016.

❖ Informes

Abogacía Española, "Cloud computing. Una guía de aproximación para la abogacía", *Guías TIC*, 2012.

Abogacía Española, "Cómo gestionar una fuga de información en un despacho de abogados", *Guías TIC*, 2016.

Abogacía Española, "Guía de Ciberseguridad y Reputación Online para Despachos de Abogados", *Guías TIC*, 2012.

Abogacía Española, "Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal", 2012.

Consejo General de la Abogacía Española, "Plan Estratégico Abogacía 2020", 2017.

INCIBE, "Decálogo ciberseguridad empresas. Una guía de aproximación para el empresario", 2017.

International Telecommunication Union, "Global Cibersecurity Index (GCI) 2017", 2017.

Logicforce, "Law Firm Cyber Security Scorecard", 2017.

NetDiligence, "2017 Cyber Claims Study", 2017.

❖ **Resoluciones**

"Advisory Opinion 2012-13/4", New Hampshire Bar Association, 2012.

"Formal Opinion nº 2015-193", The State Bar of California Standing Committee on Professional Responsibility and Conduct, 2015.

"Legal Ethics in a Digital World", CBA Ethics and Professional Responsibility Committee, 2015.

"Resolution 105A, Commission on Ethics 20/20", American Bar Association, Abril 2012.

"Review of the Australian Solicitors' Conduct Rules", Law Council of Australia, 2018.

❖ **Revistas jurídicas y tecnológicas**

Kroll, K.M., "Cyber Coverage: Separate policy, certain provisions needed for data protection", *ABA Journal*, 2016.

Ries, D., "Cyber Security for Attorneys: Understanding the Ethical Obligations", *Law Practice Today*, Marzo 2012.

Velasco Núñez, E., "Fraudes informáticos en red: del *phising* al *pharming*", *La Ley Penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, nº 37, 2007.

VV.AA., "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", *Systems, cybernetics and informatics*, volume 3, número 1, 2014.

❖ **Recursos web**

Dans, E., "Ciberseguridad: mucho que replantear", *HP Business Blog*, 15 de julio de 2016.
Disponible en: https://blog.ext.hp.com/t5/BusinessBlog-es/Ciberseguridad-mucho-que-replantear/ba-p/6922

INCIBE, "¿Estás preparado para hacer frente a una fuga de datos?", *Blog*, 2017.
Disponible en: https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

Pérez Bes, F., "La ciberseguridad en la deontología del abogado", *Abogacía Española*, 25 de mayo de 2017.
Disponible en: http://www.abogacia.es/2017/05/25/la-ciberseguridad-en-la-deontologia-del-abogado/