Vicente J. Navarro Marchante, Profesor Contratado Doctor de Derecho Constitucional de esta Universidad,

EXPONE:

En cumplimiento de lo establecido en el Reglamento de enseñanzas oficiales de máster universitario de la Universidad de La Laguna, doy el visto bueno a la presentación del trabajo realizado por D. Fabrizio Imanol Funegra Ugalde con el título "La evolución del derecho fundamental de protección de datos y su debido cumplimiento por los despachos de abogados profesionales", con la calificación de:

Notable 7.

El TFM hace una exposición adecuada de la normativa aplicable, así como de la jurisprudencia más relevante, señalando los principales problemas que se suscitan y aportando unas soluciones razonadas en Derecho.

En La Laguna, a 9 de marzo de 2019.

TRABAJO DE FIN DE MÁSTER

MÁSTER ABOGACÍA IV CURSO 2018-2019 (Convocatoria de marzo)

La evolución del Derecho Fundamental de Protección de Datos y su debido cumplimiento por los Despachos de Abogados Profesionales

Autor: Fabrizio Imanol Funegra Ugalde

Tutor: Vicente Jesús Navarro Marchante. Profesor del Área de Derecho Constitucional de la Universidad de La Laguna

Martes 26 de febrero de 2019

ÍNDICE:

1. INTRODUCCIÓN

Es conveniente empezar hablando sobre qué es lo que se entiende como dato, para saber porque merece esta especial protección dentro de la Constitución Española. El dato es toda información sobre una persona física identificada o identificable. La protección sobre estos se dará a cualquier tipo de dato sea íntima o no, que permita su identificación y que este en conocimiento o tratamiento de terceros. Por lo cual, se puede observar que el dato es un elemento bastante amplio, de gran valor ya que puede identificarnos ante la sociedad.

En la actualidad, la protección de datos ya se encuentra consolidada en nuestra sociedad como derecho fundamental, en concreto en el Art. 18.4 CE. Esto se debe a la necesidad de adaptarnos a la realidad político-socio-jurídico del momento. Ya que los datos se usan de manera lucrativa, y nace la necesidad de crear un marco normativo más sólido que garantice el derecho a la protección de datos personales.

En este nuevo siglo la tecnología está evolucionando tan rápidamente que, para asegurar una tutela efectiva de los derechos de los ciudadanos europeos, se debe ajustar esas reglas. Tras cuatro años de trabajo, el día 14 de abril de 2016 el Parlamento Europeo adoptó el Proyecto y el 27 de abril de 2016, se adoptó el Reglamento (UE) 2016/679 del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD) ha derogado la Directiva 95/46 CE a fin de reformar la normativa ya existente para adaptarla al nuevo contexto político-socio-jurídico.

"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial"[1]. Estos avances requieren un marco normativo más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de

[1] Considerando 6 Reglamento (UE) 2016/679 del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales.

Como lo explica el citado reglamento, *"el tratamiento de datos personales debe estar concebido para servir a la humanidad ya que el Derecho a la Protección de Datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".*[2]

El principal propósito de este trabajo será, por un lado, plantear los aspectos centrales del RGPD que ha comenzado a aplicarse a partir del 28 de mayo de 2018, y de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPD), con objeto de visualizar los cambios a los que se enfrenta la normativa actual. Para ello, se hará primeramente énfasis en el desarrollo normativo respecto del cual, se cuenta con abundante información que nos permitirá ver el escenario vivido en esa época hasta la actualidad. A la vez que, se hace un análisis histórico evolutivo del derecho a la intimidad, vinculado a la protección de datos personales, y que nos llevó al surgimiento de distintos mecanismos de tutela para hacer frente a los nuevos peligros y amenazas derivadas de la tecnología de la época. Construyendo así, el concepto de protección de datos el cual se irá haciendo patente conforme se avance en explicar a grandes rasgos la realidad jurídico-social en el recorrido hacia el reconocimiento y los nuevos ámbitos de protección del citado derecho.

Por lo que, la primera parte del trabajo será exponer los aspectos normativos considerados de mayor relevancia respecto a la protección de datos y su desarrollo como derecho fundamental.

Por otro lado, en la segunda parte se abordará el estudio de cómo afecta la protección de datos tras la entrada en vigor del RGPD y la nueva LOPD, a la labor del abogado como responsable de los datos personales de sus clientes. Debido a que, la protección de datos es un área de alta implicación y responsabilidad para los despachos de abogados ya que, en base al tipo de datos que gestionan son los primeros interesados en cumplir con la ley y proporcionar el máximo de garantías a sus clientes respecto a la confidencialidad y a la seguridad de datos de los clientes, al deber de secreto profesional, la responsabilidad proactiva en el tratamiento de los datos y las medidas de seguridad que debe adoptar un despacho. Para ahondar finalmente en las consecuencias de no cumplir con la actual normativa y del especial cuidado que se tiene que dar cuando se tratan datos de menores.

[2] Considerando 4 RGPD

2. MARCO NORMATIVO

2.1 ANTECEDENTES NORMATIVOS EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS: EVOLUCIÓN HISTÓRICA EN ESPAÑA

La primera redacción del art. 18.4 publicada en el BOC el 5 de enero de 1978, fue la siguiente: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos"* [3] sufriendo esta redacción algún que otro cambio hasta su redacción final.

Al principio hubo diversas propuestas de modificación, como, la defendida por el sr. Gastón Sanz del Partido Socialista de Aragón: *"Le ley limitará el uso de la informática y de cualquiera otros procedimientos que pudieran dañar el honor y la intimidad personal y familiar de los ciudadanos",* [4] centrándose en limitar la tecnología o cualquier otro procedimiento que pueda vulnerar el honor y la intimidad, entendiendo que la vulneración de derechos no sólo podía serlo por el uso inadecuado de la informática.

Por otra parte, la enmienda número 117 del grupo parlamentario de Minoría Catalana propuso la siguiente redacción: *"4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal de los ciudadanos y el pleno ejercicio de sus derechos",* [5] añadiendo que la informática también podía afectar al ejercicio de los derechos fundamentales.

El 5 de mayo de 1978 se dio el primer debate parlamentario sobre el Anteproyecto de Constitución redactado que acabo con el triunfo de la enmienda propuesta por el grupo parlamentario Minoría Catalana, la propuesta se aprobó por unanimidad y el debate quedó cerrado y listo para el dictamen del Senado.

Ante el Senado, es importante destacar la intervención de Zarazaga Burillo del Grupo Mixto y Partido Aragonés Regionalista que dijo: *"Señor Presidente, señoras y señores Senadores, este voto particular*

[3] Uno de los antecedentes que sin duda influyó sobre el Constituyente Español en la composición de este artículo relativo a la regulación de los datos personales y la informática fue la redacción del artículo 35 de la Constitución de Portugal de 1976, el cual establecía: 1. Todos los ciudadanos tendrán derecho a tener conocimiento de lo que conste en forma de registros automatizados acerca de ellos y de la finalidad a que se destinan las informaciones, y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá usar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3. Se prohíbe atribuir un número nacional único a los ciudadanos.

[4] http://lopdyseguridad.es/a-proposito-de-las-citas-en-exposiciones-de-motivos/

[5] Ídem

pretende cambiar el texto del Congreso que dice: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos », por el siguiente: «Para garantizar el honor y la intimidad personal, familiar y social de los ciudadanos y el pleno ejercicio de sus derechos, la ley limitará la utilización de la informática y otros procedimientos o técnicas que puedan atentar contra los citados derechos››. Cuando hace unas semanas defendimos en la Comisión esta enmienda, hoy convertida en voto particular, pretendimos dar a conocer nuestra opinión de que los textos legales deben ir delante de los acontecimientos sociales y asimilar los nuevos descubrimientos de la ciencia y de la técnica (...). En el espacio de tiempo que ha transcurrido hasta este debate, se ha constituido en esta misma Cámara una Comisión de investigación de las escuchas telefónicas en el Consejo General Vasco, y además, como señalan los medios de comunicación, ha estallado un pequeño «Watergate» alrededor de unos procedimientos que evidentemente entran en el contenido de este artículo, aunque como señalábamos en nuestro voto particular, desborda el entorno personal y familiar y penetra, naturalmente, en el ambiente social. Para ser previsores, tenemos que situarnos en el futuro, porque vendrán, además de los «niños probeta›› y el «niño clónico», que ya comentamos en el debate de la Comisión, otras escuchas telefónicas o vendrán otros procedimientos para poner en práctica, por ejemplo, la capacidad de transmisión de mensajes por ondas luminosas en lugar de hacerlo por ondas eléctricas o radioeléctricas, que son las que se usan actualmente, y que van a aumentar nada menos que mil veces la capacidad de los canales de comunicación. Además, vendrán otras muchas técnicas –no sólo la informática-, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera, aun antes de haber salido de la meta". "Estas nuevas técnicas que he mencionado, son, en verdad, como llamadas de atención de que el futuro está ya aquí, mientras nosotros nos seguimos moviendo en disquisiciones decimonónicas".[6]

Sin embargo, sus palabras no tuvieron el impacto suficiente en el Senado y ninguna enmienda de las propuestas en el Senado en relación con el art.18.4 del anteproyecto de Constitución Española prosperó. Para finalmente, el 28 de octubre de 1978 ser aprobado el texto tras votarse en referéndum convocado y aprobado por los ciudadanos españoles, quedando así instaurado el nuevo período constitucional español que regularía el art.18.4 en materia de protección de datos personales.

[6] Diario de Sesiones del Senado, número 60, 1978, pág. 2981 y ss. El texto íntegro en formato PDF puede consultarse en la página web: http//www.congreso.es/public_oficiales/L0/SEN/DS/S_1978_060.PDF

No sería hasta el año 1992 que España contaría con una legislación capaz de desarrollar el apartado 4 del artículo 18 referido a la protección de datos personales. Hasta ese momento la protección de los datos personales de las personas en ausencia de una ley interna que la desarrollara se garantizaban con la Ley Orgánica 1/1982 de 5 de mayo, de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, pero fue realmente insuficiente para dar respuesta ante todos los avances tecnológicos que se estaban presentando.

Con la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en adelante LORTAD) se crea un importante andamiaje institucional capaz de hacer frente a tales avances tecnológicos y de desarrollar y proteger lo que ahora se denomina libertad informática, protección de datos personales o, simplemente, autodeterminación informativa. Con la LORTAD finalmente se da cumplimiento en España al mandato constitucional del artículo 18.4 CE y a las obligaciones internacionales contraídas por España tras la ratificación del Convenio 108 del Consejo de Europa.

Debido a que el Gobierno de turno tuvo que sacar el proyecto de ley adelante tras el sonado escándalo producido en enero de ese mismo año. En el que se descubrió por la policía de una red que traficaba con datos personales procedentes "presuntamente" de ficheros automatizados de titularidad pública, lo que hizo que saliera adelante, de una vez por todas, la promulgación de la LORTAD. Aunque, el empujón definitivo al Gobierno para la presentación de esta normativa en las Cortes Generales vino dado, fundamentalmente, por tres documentos de importantísima trascendencia en el ciclo de la protección de datos en España.

En primer lugar, el Convenio de Europa de 28 de enero de 1981, para la Protección de Personas con relación al Tratamiento Automatizado de Datos de Carácter Personal ratificado por España el 27 de enero de 1984.

En segundo lugar, el acuerdo de Schengen de 14 de junio de 1985, relativo a la supresión gradual de los controles entre las fronteras comunes, que contempla el funcionamiento del llamado Sistema de Información Schengen, complejo y eficaz sistema de tratamiento de datos personales de que se sirve Europa especialmente para fines policiales y de seguridad, que supone que todos los Estados partícipes se comprometen a intercambiar información con las diferentes policías siempre que éstas cuenten con una normativa interna que brinde un nivel de protección adecuado cuando menos igual al previsto en el Convenio 108.

Finalmente, la propuesta de Directiva del Consejo de la Comunidad Económica Europea (en adelante CEE) de 24 de septiembre de 1990, relativa a la protección de las personas en lo relativo al tratamiento de datos personales (hoy Directiva 95/46 CE del Parlamento Europeo y del Consejo de Europa de 24 de octubre de 1995).[7]

El objetivo de esta Directiva de carácter vinculante era crear un marco comunitario destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, para así impulsar y favorecer el comercio intracomunitario. Sin embargo, los objetivos de la Directiva no pueden alcanzarse si previamente no se armoniza el nivel de protección que ofrecen las distintas legislaciones de los Estados miembros en lo relativo a la protección del derecho de la intimidad frente al uso de la informática. Y era necesario debido a las grandes diferencias que existían entre las legislaciones nacionales en la materia Así lo expresaba la Directiva: *"La aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan, sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección de la Comunidad"*.[8]

La incorporación de la Directiva 95/46 CEE al ordenamiento jurídico español produjo cambios radicales, al grado de que hizo necesario la adecuación de la normativa interna vigente en ese momento (LORTAD), lo que acabo con una legislación totalmente nueva acorde a los principios de la Directiva, la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal que estuvo vigente hasta finales de 2018.

Por otra parte, el Código Penal español de 1995 (modificado en 2015) había tipificado, por primera vez, supuestos delictivos que se refieren a lesiones de la autodeterminación informativa o de la intimidad en los artículos 197 y siguientes.

2.2 LA NUEVA REGULACIÓN EUROPEA: EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Es cierto que la aplicación de la Directiva alcanzo grandes objetivos, por un lado, garantizar un alto nivel de protección de los datos de carácter personal, y por otro, eliminar cuantos obstáculos pudiesen plantearle a libre circulación de esos datos. Sin embargo, parece ser que no ha resultado suficiente y por eso desde el 25 de mayo de 2018 es de aplicación el Reglamento Europeo de Protección de Datos,

[7] Hoy Directiva que ha sido derogada por el RGPD
[8] Considerando 10 Directiva 95/46/CE

norma jurídica de derecho comunitario con alcance general y eficacia directa, aplicable en todos los Estados miembros de la Unión y que no necesita ninguna norma jurídica interna para que se complete su eficacia plena.

Así, desde el 25 de mayo de 2018 la regulación del derecho a la protección de datos es uniforme en la Unión Europea, ya que la Directiva no logro eliminar las diferencias apreciables en la protección de los derechos de los ciudadanos. El RGPD se funda en la necesidad de establecer un marco uniforme más sólido y coherente para la protección de datos en la Unión Europea, como una respuesta a la rápida evolución tecnológica debido a que la recogida y el intercambio de datos personales han aumentado de manera exponencial en los últimos años.

Y es que la tecnología ha hecho posible que las empresas privadas o públicas utilicen datos personales en una escala sin precedentes al realizar sus actividades, también, las personas físicas difunden un volumen de información cada vez mayor, todo esto debido a que la tecnología ha cambiado tanto la economía como la vida social.

Entre las principales novedades del RGPD respecto a la LOPD, podemos destacar a grandes rasgos los siguientes:

1) Se aplicará a todos aquellos que traten datos personales de ciudadanos de la UE, independientemente del país en el que estén localizados.

2) Requisitos adicionales en cuanto a la información que debe proporcionarse a los clientes/interesados: Base jurídica o legitimación del tratamiento; plazo o criterios de conservación de la información; los datos del responsable del tratamiento, los datos del Delegado de Protección de Datos (si los hubiere); la finalidad; los derechos que puede ejercer así como el derecho a presentar una reclamación ante las autoridades de control, la previsión de cesiones o transferencias a terceros países, así como cualquier información adicional en el caso de los datos no se obtengan por el propio interesado.

3) Aumento de los conocidos derechos ARCO que puede ejercitar el cliente/interesado ya que hasta ahora se conocían: Añadiéndose a los citados derechos: 1) Derecho de limitación del tratamiento: El cliente puede obtener del responsable del tratamiento la limitación del tratamiento de los datos y 2) Derecho a la portabilidad: Podrá ejercerse por el interesado respecto de los datos que hubiera facilitado al responsable del tratamiento, para que este le transmita sus datos a otro responsable del

tratamiento o al mismo interesado, mediante un formato estructurado de uso habitual y de lectura mecánica, cuando el tratamiento se efectúe por medios automatizados.

4) El consentimiento debe ser una manifestación de voluntad, libre, especifica, informada e inequívoca.

5) Se exige por parte de los responsables y encargados del tratamiento una actitud consciente, diligente y proactiva (responsabilidad proactiva) en relación al tratamiento de todos los datos personales que tratan.

6) Obligación de poner medidas preventivas de protección de datos: Como la "Evaluación de impacto sobre la Protección de Datos" (EIPD) que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento.

7) Obligación de implantar medidas técnicas y organizativas más estrictas: Respecto a las medidas organizativas puedes ser la contratación de un Delegado de Protección de Dato o integrar un Sistema de Control del Riesgo, y respecto a medidas técnicas implementar la privacidad por diseño.

8) Deber de informar sobre brechas de seguridad: Impone al responsable del tratamiento de los datos el deber de notificar de la quiebra a las autoridades sin dilación alguna, y dentro de las 72 horas siguientes en las que el responsable tuvo constancia de la quiebra.

9) Mayores sanciones económicas por incumplimiento: Pudiendo llegar las más altas hasta el 4% de los beneficios globales o 20 millones de euros, cualquiera que sea la cifra más alta.

2.3 LA NUEVA LOPD EN ESPAÑA

En el caso de España, la adaptación de nuestra legislación al RGPD hizo necesaria la elaboración de una nueva LOPD. Para así poder adaptarse a lo establecido por el RGPD, a su vez el art. 18.4 CE se ejercerá con arreglo a lo dispuesto en el RGPD y a esta nueva ley orgánica. Los aspectos más importantes a destacar de esta nueva normativa en relación con la anterior son:

1) En primer lugar, la regulación de los datos referidos a las personas fallecidas respecto a lo cual no se hace mención alguna en el RGPD. No obstante, en esta nueva LOPD se da un paso más, y se permite que no solamente los herederos, sino también los albaceas testamentarios los que puedan solicitar el acceso a los mismos, así como su supresión o rectificación, en su caso siempre con sujeción a las instrucciones del fallecido.

2) Un nuevo derecho de rectificación y supresión: Ya no solamente se limita a la exactitud de la información publicada o su veracidad, sino que entra también en el área de la intimidad y el honor.

3) En cuanto a régimen sancionador, la nueva LOPD describe las conductas típicas, diferenciando entre sanciones leves, graves y muy graves, tomando en consideración la distinción que hace el RGPD al fijar la cuantía de las sanciones.

4) La edad en la que los menores pueden dar su consentimiento por sí mismo se reduce a 13 años. Y al igual que lo que dice el Art.4.11 RGPD tiene que ser un consentimiento toda "manifestación de voluntad libre, especifica, informada e inequívoca por la que este acepta" mediante una declaración o una clara acción afirmativa.

5) La importante figura del DPD queda también plasmada en la nueva LOPD, partiendo de que esta figura puede ser voluntaria u obligatoria, formar parte o no de la organización/estructura del despacho y puede ser tanto persona física como jurídica. Lo que la nueva LOPD establece es un *numerus clausus* de supuestos en que si procede su nombramiento.[9]

3. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

3.1 CONSIDERACIONES PREVIAS

A lo largo de la historia la situación del derecho a la intimidad ha ido variando considerablemente en virtud del desarrollo tecnológico y hoy no se puede negar que ha habido un cambio de dirección en el ámbito de protección, donde además de tener el individuo la facultad de rechazar invasiones de todo tipo en su ámbito privado, ahora supone para cada uno el reconocimiento de un derecho de control sobre toda información relativa a su persona. *"Por esto, el uso y control sobre los datos concernientes a cada persona, ya no solamente debe ser tenido en cuenta como una mera prerrogativa, sino que además debe entenderse como un nuevo derecho fundamental capaz de hacer frente a las nuevas agresiones que ha traído consigo este avance tecnológico".*[10]

Y este cambio de dirección es posible debido a que los derechos fundamentales se han caracterizado a lo largo de la historia por su amplitud y apertura a nuevas formas. Tanto la doctrina como la jurisprudencia constitucional afirman la presencia de un catálogo de derechos fundamentales abierto,

[9] Guía GT29 "Directrices sobre los delegados de protección de datos"
[10] Ídem

reemplazando la visión atemporal de estos. Para así poder adaptarse y dar una respuesta eficaz a las demandas de los ciudadanos debido al constante progreso y evolución informática.

Como dice, Norberto Bobbio *"los derechos humanos son derechos históricos que surgen gradualmente y no todos a la vez y para siempre"*[11]. Por lo que, los derechos no pueden quedarse como, un producto inmóvil, estativo, perenne, sino dinámico, fluido y cambiante para así poder dar respuestas a las nuevas demandas individuales de los ciudadanos derivadas de una sociedad informatizada y en continuo progreso.

3.2 COMO DERECHO DE 3º GENERACIÓN

El paso de las distintas etapas de la historia ha determinado la aparición de las "generaciones de derechos". Y es en la "tercera generación de derechos" donde se aprecia con mayor claridad la influencia de los avances tecnológicos y científicos, tomando también mayor importancia el reconocimiento del derecho a la intimidad. Por lo que podemos hablar de un antes y un después de este derecho, un cambio necesario para dotar de protección, a esas nuevas categorías de derechos a la que una parte de la sociedad clama reconocimiento y tutela.

Los derechos de la persona, como aclara Norberto Bobbio *"(...) no nacen todos en un momento. Nacen cuando deben o pueden nacer. Nacen cuando el aumento del poder del hombre sobre el hombre, que acompaña inevitablemente al progreso técnico, es decir, al progreso de la capacidad del hombre de dominar la naturaleza y a los demás, crea nuevas amenazas a la libertad del individuo o bien descubre nuevos remedios a su indigencia: amenazas que desactivan con exigencias de límites al poder; remedios que se facilitan con la exigencia de intervenciones protectoras del mismo poder (...)".*[12]

3.3 INTIMIDAD COMO PASO PRELIMINAR AL DERECHO DE DATOS

El derecho a la intimidad engloba todo lo que es propio de la persona, entendiendo esto como la información que mantiene para sí mismo. Se trata de lo que cada persona quiere mantener en su esfera privada sin que nadie tenga acceso a ella. "*El derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, el poder de resguardar su vida privada de una publicidad no requerida, y así lo ha dicho este Tribunal" (STC 134/1999 y STC 115/2000)*

[11] **BOBBIO**, Norberto, "El tiempo de los derechos", Editorial Sistema, Madrid, España, 1991, pág. 68
[12] http://www.sideme.org/doctrina/articulos/art001121-pe.htm

Desde un punto de vista jurídico, la intimidad es la respuesta del derecho al interés de cada persona en lograr un ámbito en el que sea capaz de desarrollar, sin intrusión, curiosidad o indiscreción ni injerencias de los demás, su vida privada. Pero a la vez entiendo que todo esto resultaría insuficiente en la actual sociedad, ya que no se puede contemplar solamente la intimidad desde este estatus negativo, sin contemplarla al mismo tiempo, como un derecho de control sobre la información que afecta a cada sujeto.

Por lo tanto, se ve como poco a poco deja de ser un derecho de no interferencia para encontrarse con una faceta positiva de control, de decisión y de vigilancia por parte del titular de su intimidad.

No cabe duda que la intimidad ha formado parte estructural en la construcción de la doctrina que sustenta el derecho a la protección de datos personales; pero como señala el Tribunal Constitucional que *"el derecho fundamental a la intimidad (Art. 18.1 CE) no aporta por sí solo una protección suficiente frente a la realidad derivada del progreso tecnológico y la informática" (STC 292/2000).* El constituyente era consciente de los riesgos que traía consigo el "uso de la informática" y encomendó al legislador incorporar un instituto de garantía *"como forma de dar respuesta a una nueva amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993).*

Miguel Castaño nos ilustra al decir que *"(...) aun cuando la intimidad pudiera considerarse muy relacionada con el secreto, esta noción debe ser depurada, ya que no es cierto que cuanto menos se sepa de nosotros, gocemos de una mayor intimidad, ya que esta no es simplemente la ausencia de información sobre cada uno en la mente de los demás, sino más bien el control que podemos ejercer sobre nuestra propia información personal"*[13]

Es imposible negar que, independientemente del "nomen iuris" que se utilizare, privacidad o intimidad han jugado un papel preponderante y decisivo en la compresión, construcción y evolución del concepto de protección de datos personales, un concepto que décadas más tarde y con la práctica de su protección se iría desmarcando de esa línea teórica inicial de la cual derivó para convertirse en un auténtico derecho fundamental con autonomía propia.

3.4 LA EVOLUCIÓN CONCEPTUAL: DE LA INTIMIDAD A LA PROTECCIÓN DE DATOS PERSONALES COMO DERECHO AUTÓNOMO

[13] **MIGUEL CASTAÑO,** Adoración de, "Libertad de información y derecho de intimidad: medios para garantizarla. Incidencia en el ámbito de la estadística, REDUC, número 12, septiembre de 1986, pág. 175.

La irrupción de la informática y el manejo descontrolado de los datos de las personas, supuso para los juristas la difícil tarea de encuadrar en alguna categoría jurídica protegible existente, y fue en la intimidad en donde se encontró la respuesta jurídica adecuada. Es en la intimidad donde se ubica de manera más idónea la tutela de las personas frente al uso de los datos informatizados.

Fue así como nace en el ordenamiento jurídico español el derecho a la protección de datos de carácter personal que dice así en el Art. 18.4 CE *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Y surge como derecho o libertad fundamental, para así poder hacer frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes de un uso ilegítimo del tratamiento mecanizado de datos, *lo que la Constitución llama "la informática", por lo que se dio en llamar "libertad informática" (STC 202/1999).*

"Esta llamada "libertad informática" se definió como el derecho de controlar el uso de los mismos datos insertos en un programa informático (habeas data), comprendiendo el derecho a la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel que justificó su obtención" (STC 11/1998).

Por lo que se entiende que, ante la nueva agresión al derecho a la intimidad, debido a, las nuevas tecnologías, es lógico pensar que habría que cambiar los mecanismos de protección existentes. De esta manera, se forma el derecho a la protección de datos, como un "nuevo traje" que reconocía un poder de disposición y de control sobre los datos personales para decidir qué datos se proporcionaran a terceros, sean las Administraciones Públicas o un particular, o cuales puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Por su parte, Murillo de la Cueva recuerda *"la estrecha vinculación o conexión que existe entre el derecho a la intimidad y el derecho a la protección de datos personales, pues a su parecer es a partir de la primera que se construye la segunda. Sin embargo, está a favor de separar el derecho a la autodeterminación informativa del derecho a la intimidad, señalando que… no coinciden los ámbitos que se quieren defender con el derecho a la intimidad y con la protección de datos personales".*[14]

[14] **LUCAS MURILLO**, Pablo "El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática", Editorial Tecnos, 1990, pág. 120

El derecho de protección de datos no se centra de manera exclusiva en lo que se entiende como intimidad en sentido estricto. Su distinción radica en su objeto y contenido, pues por un lado la función del derecho fundamental a la intimidad art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y las intromisiones de terceros en contra de su voluntad [15]. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un "poder de control" sobre sus datos personales, sobre su uso y destino con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

De esta manera, el objeto de protección del derecho a la protección de datos va más allá protegiendo todo tipo de datos que revelen aspectos de la vida de una persona, no solamente los que afecten al derecho a la intimidad, sino también a cualquier otro derecho. De esta forma, el derecho a la protección de datos pasa a configurarse como un derecho autónomo, rompiendo ese lazo que de mucho tiempo atrás, une el derecho a la intimidad con el derecho a la protección de datos personales; y así lo haría más tarde el propio Tribunal Constitucional al decir *"que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico" (STC 292/2000).*

4. EFECTOS SOBRE LA ACTIVIDAD DEL ABOGADO

4.1 ¿CÓMO DEBO INFORMAR AL CLIENTE EN LA RECOGIDA DE DATOS Y DEL EJERCICIO DE SUS DERECHOS RELATIVOS A LA PROTECCIÓN DE DATOS?

El principio de transparencia exige que toda información dirigida al público o al interesado sea *"concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo y, además, en su caso"*[16]. Por ello el profesional debe diseñar políticas concisas, transparentes, sencillas y accesibles para comunicar al cliente los detalles del tratamiento y el ejercicio de los derechos sobre sus datos.

La información puede ser facilitada por escrito o por medios electrónicos y si el cliente lo solicita, la información puede darse de forma oral, siempre que se pueda demostrar la identidad del cliente por otros medios.

[15] Sentencia del Tribunal Constitucional 144/1999
[16] Considerando 58 RGPD

Toda información que el profesional este obligado a facilitar al cliente debe ser gratuita, tanto si se refiere a la información sobre el tratamiento de datos como al ejercicio de derechos, excepto cuando sean manifiestamente infundadas, excesivas o repetitivas pudiendo en este caso: a) Cobrar una tasa razonable basada en los costes administrativos o b) Negarse a actuar respecto a lo solicitado. Será el profesional el que deba demostrar que las solicitudes son infundadas o excesivas.

Según el Art. 11 LOPD, entendemos que en nuestra labor de abogados debemos cumplir ineludiblemente con la siguiente información:

-Identidad y datos de contacto del responsable o DPD, en caso de existir.

- Fines del tratamiento y base jurídica del tratamiento

-Plazo de conservación o criterios que lo determinen

-De sus derechos ARCO y los añadidos de limitación y portabilidad

-Derecho a presentar una reclamación ante la AEPD

-Derecho a retirar el consentimiento

-Posibles transferencias o cesiones, y sus destinatarios

-Posibles consecuencias de no facilitar sus datos

-Los intereses legítimos del responsable o la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

Y si la información no ha sido facilitada por nuestro cliente:

-Las categorías de datos tratados

-Las fuentes de procedencia de los datos[17]

Como se ha comentado, lo normal será recabar estos datos tras una entrevista o conversación telefónica, siendo lo más habitual recogerla en un formulario en papel, o como anexo a la hoja de encargo profesional. Una vez se haya informado al cliente, no será necesario volver a hacerlo.

[17] Artículo 11 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD).

Los despachos pueden diseñar formularios de información para los clientes de dos maneras que se denominan "información por capas", en el primer nivel se dará la información básica de forma resumida en el momento en que se recojan sus datos, mientras que en el segundo nivel es donde se presentará detalladamente el resto de la información. Esta información también estará disponible en la página web del despacho.

4.2 ¿CÓMO DEBO OBTENER EL CONSENTIMIENTO PARA EL TRATAMIENTO Y CESIÓN DE LOS DATOS DEL CLIENTE?

Respecto al consentimiento, como se dijo anteriormente este debe ser una manifestación de voluntad, libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen[18]. Este debe ser informado, en un lenguaje claro y sencillo, evitando de cláusulas abusivas o confusas.

La nueva LOPD establece que para el tratamiento de datos de carácter personal el consentimiento se ha debe dar forma explícita, ya no cabe la aceptación tácita como ocurría con la antigua LOPD, pues el silencio, las casillas ya marcadas o la inacción no constituyen consentimiento ya que no son consideradas como una *"clara acción afirmativa".*[19]

Sobre el responsable recae la prueba del consentimiento, este debe demostrar que ha obtenido el consentimiento para tratar los datos del interesado de la manera que establece el RGPD. Este deberá ser consciente y libre, por lo que no será lícito si se condiciona a una prestación de servicios sin ser necesario para su realización. Los consentimientos que infrinjan, aunque sea de manera parcial el RGPD han de ser considerados nulos.

4.3 ¿Y NECESITO AUTORIZACIÓN/CONSENTIMIENTO PARA TRATAR DATOS DE LA PARTE CONTRARIA?

Los abogados además de los datos de sus clientes tratan datos de las partes contrarias en los procesos judiciales. En estos casos se produce una colisión entre derechos fundamentales: Por una parte, el derecho a la protección de datos del Art. 18.4 CE y el derecho de defensa y a la asistencia letrada, como manifestación del derecho a obtener una tutela judicial efectiva del Art. 24.2 CE.

[18] Artículo 6 LOPD
[19] Considerando 32 RGPD

Partiendo de la consideración de que el derecho a la protección de datos y a la intimidad no es absoluto, "*como no lo es ninguno de los derechos fundamentales" (STC 186/2000),* la AEPD ha entendido que debe darse una prevalencia al derecho del Art. 24.2 CE, ya que, si los abogados solicitan el consentimiento a la parte contraria o les comunican determinada información procedente de los propios clientes, podrían perjudicar claramente a su derecho a obtener la tutela judicial efectiva.

Para fundamentar la prevalencia del derecho a la defensa del cliente frente a los derechos de protección de datos de la contraparte nos remitimos al informe del año 2000-0000 de la AEPD que dice:

"(...) El legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida. En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquellos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 CE.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquel el almacenamiento de la información necesaria para que el cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de "los medios de prueba pertinentes para su defensa", vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho. Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes, por lo existirá, desde el punto de vista de la

Agencia, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 CE y sus normas de desarrollo".[20]

4.4 EL DEBER DE SECRETO

El secreto profesional impone límites específicos a la comunicación de datos a los juzgados y tribunales, a la propia parte y a la contraria, así como a sus defensores o representantes. También tiene implicaciones en los ejercicios de derechos por la contraparte frente a abogados y procuradores.

Esta obligación se extiende también a los miembros del despacho de abogado afectado (secretarias/os, pasantes y colaboradores), al igual que en el caso de que se ejerza la abogacía de manera colectiva, el deber de secreto se ha de extender a estos.

El secreto profesional es uno de los deberes básicos que rige en el ejercicio profesional de abogado, la plasmación de este deber de los abogados está establecida en la LOPJ que dice:

"Los abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquier de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos" (Art. 542.3 LOPJ).

El abogado no estará obligado a informar a la contraparte de qué datos concretos trata de ella en un proceso judicial ya que eso podría afectar a nuestro derecho de defensa o secreto profesional. Aunque, si debe atender su solicitud sobre qué datos trata o cuando ejerza de los derechos de acceso y cancelación, indicando en la contestación que trata datos de ella y el procedimiento o asunto, y que prevalece el derecho de defensa y secreto profesional para no facilitar más datos.

Este deber se tiene que entender en sentido amplio y no solamente a las confidencias y propuestas de nuestro cliente, sino también a las del adversario, la de los compañeros y todos los hechos y documentos de que tengamos noticia por razón de cualquier de las modalidades de nuestra actuación profesional.

El Estatuto General de la Abogacía Española (en adelante EGAE) establece que es deber del abogado *"mantener como materia reservada las conversaciones y correspondencia habidas con el abogado o abogados contrarios, con prohibición de revelarlos o presentarlos en juicio sin su previo*

[20] Informe 2000-0000 AEPD que trata sobre "Tratamiento por Abogados y Procuradores de los datos de las partes en un proceso" y que se puede obtener información en el siguiente enlace: https://ayudaleyprotecciondatos.es/2013/02/07/tratamiento-abogados-datos-parte-contraria/

consentimiento" (Art. 34 EGAE). Lo que es parte confidencial porque ha sido tratado por los abogados no puede ser utilizado de ninguna manera con independencia del medio (Carta, fax, burofax o email, etc.). "*Esta prohibición abarca la grabación de conversaciones de presencia, telefónicas y telemáticas sin previa advertencia y conformidad, que quedan dentro del ámbito del secreto profesional" (Art. 5.4 CDAE).*

En igual sentido, el Código Deontológico español señala que *"el abogado no podrá aportar a los tribunales, ni facilitarle a su cliente las cartas, comunicaciones o notas que reciba del abogado de la otra parte, salvo expresa autorización del mismo" (ART. 5.3 CDAE).*

No debería ser necesario advertir de la confidencialidad de la comunicación, sin embargo, es recomendable que los abogados tengan la costumbre de insertar en sus comunicaciones con las partes una cláusula tipo, advirtiendo de la prohibición deontológica. Advertirse que en el caso de mantenerse comunicaciones con abogados de la UE si se pretende que queden vinculados al secreto debe plasmarse dicha cláusula en las comunicaciones.

También, habrá casos de suma gravedad en los que, la obligada preservación del secreto profesional puede causar perjuicios irreparables o flagrantes injusticias, "*entonces se deberá acudir al Decano del Colegio que aconsejará al abogado para orientarle o determinar medios o procedimientos alternativos de solución del problema planteado ponderando los bienes en conflicto" (ART. 50 CDAE).*

Por lo que caben, excepciones a la regla general del secreto profesional cuando: a) Se tiene autorización del abogado emisor la cual deberá ser expresa, es decir, por escrito; b) La concurrencia de causa grave, previa autorización de la Junta de Gobierno del Colegio (Art. 34 e) EGAE), a criterio colegial y en situaciones excepcionales y escasas; 3) Por la falta de vinculación modal con la defensa.

Es gracias a este deber de secreto profesional que permite a los abogados actuar con total libertad y garantía a la hora de exponer sus posturas en las negociaciones con la parte contraria sin miedo a que puedan ser usados si se produjese un juicio y que así se mantenga un ambiente de confianza que permita a las partes llegar a un acuerdo que evite el pleito.

Como se ha dicho anteriormente, es muy recomendable el uso de la hoja de encargo, y más aún pues nos puede evitar incurrir en un delito de descubrimiento y revelación de secretos tipificados en el Art.

199.2 CP. Por lo que es importante que en la hoja de encargo el cliente manifieste que los documentos que va a proporcionarnos para hacer nuestra labor han sido obtenidos de manera legal.

Resalto esto pues hay veces que los abogados tratan datos de la parte contraria, en el ejercicio del derecho de defensa y debemos tener claro que su origen es lícito para su utilización y aportación a un proceso judicial. Es de señalar lo resuelto por la AP de Las Palmas 10-06-2013:

"Que condeno a una abogada por un delito de descubrimiento y revelación de secretos del Art. 199.2 CP (...). En este caso, probada la utilización en una vista de medidas provisionales de una determinada documentación personal y reservada de la parte contraria, obtenida de manera ilícita por la cliente de la abogada (también condenada) y esposa de la parte contraria. La letrada no había tenido intervención alguna en la obtención irregular de dicho documento, sino que, con posterioridad a ello, conociendo tal circunstancia, decidió utilizarlo en la citada vista de medidas provisionales. Entiende la AP que la acción de divulgar secretos aplica a cualquier persona cuyo descubrimiento ilícito les conste, pues el abogado ostenta un específico deber de guardar sigilo respecto de este tipo de datos, impuesto por sus normas deontológicas, y especialmente por el Art. 542.3 LOPJ".[21]

4.5 RESPONSABILIDAD PROACTIVA DE LA GESTIÓN DEL RIESGO Y MEDIDAS QUE TIENE QUE TENER UN DESPACHO DE ABOGADOS PARA EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

Como se ha dicho una de las principales novedades del RGPD, es el principio de responsabilidad proactiva que consiste en que el abogado como responsable del tratamiento de datos debe tener una actitud consciente, diligente y proactiva cuando trate los datos. Implica la necesidad de que el responsable del tratamiento de datos aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos personales es conforme al Reglamento. Es decir, no basta con cumplir con la normativa de protección de datos también hay que poder demostrar que se está cumpliendo con la normativa.

A su vez, el responsable del tratamiento debe cumplir con los principios relativos al tratamiento de datos (licitud, limitación de los fines, minimización, exactitud, integridad y confidencialidad y conservación) y debe ser capaz de demostrarlo.

[21] Audiencia Provincial de Las Palmas 10-06-2013

Este principio requiere que se analicen qué datos se tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo para así determinar qué medidas son las más adecuadas para cumplir con el RGPD y demostrarlo ante las autoridades en caso de supervisión.

A continuación, se van a destacar las principales medidas de responsabilidad proactiva que deben darse en un despacho de abogados cuando trata datos.

Análisis del riesgo en los despachos

Este proceso implica realizar dos tareas principales: Identificarlos y evaluarlos. Es muy importante la identificación de las amenazas a las que un despacho puede estar expuesto en el tratamiento de los datos de los clientes pues; así tendremos en cuenta cuales son los riesgos que esa amenaza puede traer y así en calidad de responsables o encargados, aplicar las medidas tanto técnicas como organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Entendemos por riesgo toda posibilidad de que se materialice una amenaza y sus consecuencias negativas. Estos riesgos pueden situarse en tres categorías: a) Sobre los afectados, b) Sobre los riesgos corporativos y c) Sobre los riesgos de cumplimiento normativo general. Una vez se hayan verificado los riesgos, hay que determinar cuáles son las medidas técnicas que se van a implementar, teniendo en cuenta también la tipología del despacho profesional (colectivos, con o sin asociación; comunidades de bienes, sociedades civiles, sociedades mercantiles profesionales; ejercicio independiente con o sin colaboración con otros letrados, etc.). Un despacho debe asegurarse los siguientes hitos[22]:

1. Garantía de confidencialidad, integridad, disponibilidad, así como la capacidad de adaptación de sus sistemas informáticos a una crisis.

2. En caso de incidente, sea este físico (Sobrealimentación eléctrica, incendio, robo, hurto, inundación, etc.) o técnico (ataques informáticos, virus), tener y mostrar capacidad de restauración rápida y ágil de la disponibilidad y acceso a los datos personales

3. Tener establecidos controles de verificación, evaluación de riesgos y valoración regular de la eficacia de las medidas técnicas y organizativas necesarias para garantizar la seguridad del tratamiento. El despacho no solo ha de tener un programa de control que este se ajuste a las

[22] Guía práctica de análisis de riesgos pág. 31. Se puede acceder en el siguiente enlace https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

previsiones normativas, atendidas las circunstancias concurrentes y las características de la empresa, sino también que tales controles se revelen eficaces y adecuados (en contenido y potencial eficacia).

Por amenaza se entiende a todo factor de riesgo que potencialmente puede provocar un daño a los interesados titulares de los datos personales sobre los cuales el despacho realiza un tratamiento. Las amenazas pueden venir por varias vías[23]:

1) Acceso ilegítimo a los datos: El daño que se podría dar si conocen de estos datos terceros, además, del impacto que esto genera en la relación abogado-cliente.

2) Modificación no autorizada de datos: El daño que se podría dar si estos datos se dañan, alteran o corrompen.

3) Eliminación de datos: Por ejemplo, al no poder utilizar un dato por un virus y la corrupción del archivo, afectando a la disponibilidad sobre esos datos.

Por lo que para evaluar los riesgos ha de valorarse el impacto de la exposición a la amenaza junto a la probabilidad de que esta se materialice. Teniendo claro el significado de riesgo y amenaza, ahora hay que considerar el impacto o alcance de la amenaza, verificando que daños se pueden producir si tal amenaza se materializara. Así, por ejemplo, la quiebra de unos formularios internos o borradores de cláusulas del despacho sin ningún dato identificativo, tendría un impacto despreciable. En cambio, un convenio regulador de divorcio con liquidación de sociedad de gananciales, en su versión definitiva, puede ser relevante debido a los datos económico-patrimoniales que trata.

Es importante saber a qué amenazas se enfrenta un despacho, pues pueden ir desde el daño reputacional, la pérdida de clientes hasta daños económicos, todo ello por no contar con mecanismos capaces de hacer frente a violaciones de la confidencialidad o quiebras de seguridad.

Resulta fundamental al realizar el análisis de riesgo, conocer los flujos de información que tiene el despacho entre sus distintas áreas o en sus bases de datos. Para así, poder realizar el tratamiento de los riesgos la cual es la fase final de todo este proceso de gestión. Que consistirá en disminuir o minimizar la exposición al riesgo mediante un sistema de medidas de control, siempre encaminado a reducir la probabilidad que ocurra, o bien el impacto, en caso de amenaza materializada. El objetivo es mitigar

[23] Ídem pág.4

los riesgos hasta hacerlos residuales en relación al estado de la tecnología del momento ya que el riesgo cero no existe pues, la evolución tecnológica va a velocidad de crucero.

Registro de actividades de tratamiento

Con la eliminación de la obligación de notificar a la AEPD los tratamientos de datos, se crea el Registro de Actividades de Tratamiento, que no deja de ser un registro interno y categorizado de estas actividades. Lo que se pretende con la inclusión de esta figura es la efectiva responsabilidad activa de las entidades que tratan datos personales, y, por lo tanto, puedan acreditar la conformidad de su actuación con la normativa de protección de datos.

Los responsables o encargados deben mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD. "*Están exentas de llevar este registro de actividades las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales" (Art. 30 RGPD)*.

Por lo que, los despachos de abogados deberán llevar este registro de actividades, por la esencial afectación a derechos y libertades que el tratamiento de datos de sus clientes puede tener. En caso de incumplimiento en la elaboración del registro de actividades de tratamiento puede ser considerado como infracción grave.

Protección de datos desde el diseño y por defecto

Debido al avance de las nuevas tecnologías y del flujo continuo de nuestros datos, cada vez la protección de datos y la intimidad están unidas en todo el ciclo de vida de dichas tecnologías, desde el momento en el que se plantea su diseño hasta su despliegue en general. Antes, lo normal por parte de las empresas en el diseño de un nuevo producto o servicio era, sacarlo al mercado y luego analizar la cuestión legal una vez en funcionamiento; ahora lo que viene a decir el RGPD es que se debe abordar esta cuestión teniendo en cuenta las leyes de protección de datos en el momento del diseño, no después.

Se pretende que la privacidad se mantenga durante todo el tiempo que dure el servicio que ofrecemos a los clientes. "*La privacidad desde el diseño garantiza que durante la vida de instrumento*

tecnológico la información sea segura, desde el "nacimiento" hasta el "fallecimiento", desde un "extremo a otro".[24]

Este cambio de mentalidad a la protección desde el diseño, implica que labor de abogados se realice de manera proactiva y estableciendo las medidas necesarias desde el primer momento para que los riesgos no se materialicen. Para poder aplicar este principio en cumplimiento del RGPD, habrá que tener en cuenta: 1) La naturaleza, ámbito, contexto y finalidad del tratamiento; 2) Los riesgos de diversa probabilidad y gravedad; 3) Estado de la técnica y 4) Costes.

Este principio tiene su fundamentación dentro del RGPD en:

"…A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto...".[25]

"…teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contextos y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, concebidas para aplicar de forma efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados…".[26]

Evaluación de impacto sobre la Protección de Datos (EIPD)

Es una herramienta que ha establecido el RGPD debido al continuo avance de la tecnología y la evolución de los tratamientos que propician la aparición de nuevos riesgos que deben ser gestionados. Lo realiza con carácter preventivo el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de adoptar de las medidas de control necesarias para eliminar o atenuar en lo posible aquellos que se hayan identificado garantizando así el derecho a la protección de datos de los clientes.

[24] https://protecciondatos-lopd.com/empresas/privacy-by-design/
[25] Considerando 78 RGPD
[26] Artículo 25.1 RGPD

El GT29 define un riesgo como *"un escenario que describe un evento y sus consecuencias, estimado en términos de impacto y probabilidad"*[27]. Por tanto, la gestión de riesgos es el conjunto de aquellas actividades y tareas realizadas en una organización para monitorizar y controlar su exposición ante los riesgos.

El RGPD prevé que las EIPD se lleven a cabo "antes del tratamiento" en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.[28]

No siempre será necesaria la realización de una EIPD, aunque será recomendable a la hora de realizar nuevos tratamientos de datos. La nueva regulación señala que es obligatoria cuando: 1) Se dé un alto riesgo en el tratamiento de datos, 2) Evaluación sistemática, 3) Tratamiento a gran escala de datos especialmente protegidos y 4) Uso de tecnologías invasivas.

Algunas de las entidades obligadas a realizar la EIPD son: Farmacéuticas, hospitales, empresas que realicen e-commerce o colegios. No obstante, se entiende que, en el caso de los despachos de abogados al afectar su actividad a derechos y libertades de las personas físicas y poder tratar datos sobre condenas e infracciones penales o medidas de seguridad conexas, deben hacer una EIPD.

Por lo tanto, el abogado como responsable del tratamiento antes de realizar la EIPD tiene que buscar el asesoramiento del DPO del que se hablara a continuación con mayor profundidad

Delegado de Protección de Datos (DPD/DPO)

El DPD es una figura, que debe estar en disposición de ayudar a los responsables en el cumplimiento de las directrices del RGPD, gracias a sus conocimientos especializados en la normativa protectora de datos personales.

El concepto de DPD no es nuevo. Aunque en la Directiva 95/46 CE no se exigía a ninguna organización el nombramiento de un DPD, la práctica de tal designación se ha desarrollado en varios Estados miembros a lo largo de los años. Incluso antes de la entrada en vigor del RGPD, el GT29 decía que el nombramiento de un DPD puede facilitar el cumplimiento del RGPD y, además,

[27]Guía práctica de Evaluación de impacto RGPD Pág. 5. Se puede acceder en el siguiente enlace: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
[28] Ídem Pág.2

convertirse en una ventaja competitiva para las empresas[29]. Es así como el DPD se convierte en una figura fundamental en el nuevo sistema de gestión de los datos.

En virtud del RGPD, es obligatorio que algunos responsables y encargados del tratamiento designen un DPD. Así será en el caso de todas las autoridades y organismos públicos (con independencia de qué datos traten), y de otras organizaciones cuya actividad fundamental consista en la observación sistemática de personas a gran escala, o que traten categorías especiales de datos o datos personales relacionados con condenas y delitos penales.[30]

El RGPD no aclara con detalle quienes están obligados a designar un DPD, sino que da unas directrices establecidas en el Art. 37 RGPD. Y es que del concepto jurídico de "gran escala" no es posible dar una cifra exacta, dejando una gran inseguridad para los profesionales o empresas afectadas que no saben sin tienen que cumplir con esta nueva obligación, que ya esté vigente. La nueva LOPD ha intentado dar una solución con un amplio listado de todos los obligados a designar un DPD en su Art. 34. LOPD.

El GT29 recomienda tener en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala: a) el número de interesado afectados, b) el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento, c) la duración o permanencia, de la actividad de tratamiento de datos, d) el alcance geográfico de la actividad de tratamiento[31]. Como ejemplos de tratamiento a gran escala cabe citar: Hospitales, Bancos compañías de seguro, colegios profesionales, o centros educativos. En cambio, no constituyen tratamiento a gran escala "el tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado"[32] y por tanto un abogado no tendría la obligación de nombrar un DPD, pero sí que es altamente recomendable.

Por tanto, la designación de un DPD constituye una obligación siempre y cuando en el despacho se realicen operaciones de tratamiento que, en razón a su naturaleza, alcance y/o fines, precisen una observación habitual, regular y sistemática de interesados a gran escala; o, cuando haya tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. También, será obligado cuando el despacho actúe por cuenta de sus clientes en operaciones

[29] Guía GT29 pág.4 sobre "Directrices sobre los delegados de protección de datos"
[30] Ídem pág. 4
[31] Ídem pág. 8
[32] Ídem pág.9

financieras, inmobiliarias, o cuando presten los servicios de constituir sociedades, ejercer la secretaría u otros servicios afines a una sociedad.

Hay que dejar claro que los DPD no son personalmente responsables en caso de que se incumpla el RGPD. Ya que es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza conforme al RGPD[33]. Por tanto, el DPD no puede ser destituido ni sancionado por el responsable o el encargado por el desempeño de sus funciones, salvo que incurra en negligencia grave o dolo, como puede ser el caso de omisión en el asesoramiento o la mala praxis que puede implicar responsabilidades relativas al secreto y confidencialidad.

El DPD en su prestación de servicios puede ser:

a) DPD interno: Formar parte de la plantilla, desarrollando su actividad a tiempo completa o parcial. Contratado como trabajador por cuenta ajena, todas aquellas funciones ajenas al desempeño del cargo, por ejemplo, la ocupación de otras tareas del despacho se encontrará sujeta al deber de cumplimiento de órdenes e instrucciones por parte del titular del mismo (Art. 5. C) ET), salvo que supongan un conflicto de intereses para el DPD.

b) DPD externo: Como profesional externo, bajo la figura del arrendamiento de servicios. En el caso de abogados que presten servicios de DPD a otros despachos o empresas, es de gran importancia tener en su poder la acreditación de conocimiento mediante "certificaciones oficiales" que, sin ser obligatorias, aportan confianza y seguridad a los clientes que acuden al despacho respecto al tratamiento de sus datos; además de ser un aval de solvencia profesional indudable.

En su actuar debe hacerlo con total independencia[34], de forma que no reciba instrucciones en lo que respecta al desempeño de sus funciones, además de contar con los recursos suficientes para desarrollar su labor de forma efectiva. Y como se ha explicado antes, este gozará de indemnidad por el ejercicio de las mismas, pues no puede ser destituido ni sancionado por desempeñarlas (en el caso interno) ni resuelto su contrato (en el caso externo) y rinde cuentas directamente al más alto nivel jerárquico de la corporación.

Este DPD será designado atendiendo a sus cualidades profesionales, sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las

[33] Ídem pág. 5
[34] Considerando 97 RGPD

funciones que le son propias. Es recomendable que además de tener conocimientos jurídicos tenga conocimientos tecnológicos ya que la mayoría de tratamiento de datos es automatizado; y que estos conocimientos especializados a su vez concuerden con el grado de complejidad y cantidad de datos que el despacho trate.

Por último, las principales funciones dentro del despacho del DPD son:

a) Informar y asesorar, tanto al responsable o al encargado del tratamiento, empleados que se ocupen del tratamiento y al conjunto de letrados del despacho de las obligaciones que incumben al cumplimiento de la normativa.

b) Supervisar el cumplimiento normativo

c) Ofrecer asesoramiento que se le solicite acerca de la EIPD

d) Atender las peticiones de información de los interesados en el ejercicio de sus derechos

e) Cooperar con la autoridad de control y actuar como punto de contacto de la autoridad de control

4.6 FUGA DE INFORMACIÓN EN UN DESPACHO DE ABOGADOS

Dentro de, un despacho de abogados la ciber seguridad debe ser un elemento indispensable de la información en general, debe ser una prioridad y cuestión estratégica de los despachos. Al tener los despachos de abogados información sensible y confidencial, la vulneración de estos, puede acarrear para los despachos daños de carácter legal, deontológico, económico y reputacional, que han de ser evitados.

Un despacho profesional, respecto de la información y los datos personales de su cliente, debe proteger: la confidencialidad, integridad y disponibilidad. Ya que, en caso de pérdida, sustracción o acceso no consentido por parte de terceros, puede ser empleada con fines ilícito penales (extorsión), informativos (medios de comunicación), reputacional (desprestigio). Esa información confidencial, a su vez, puede ser constitutiva de bien intangible objeto de tráfico comercial en el mercado de datos, y es que los datos se han convertido en el "petróleo del siglo XXI".[35]

Por lo que las fugas de información se han convertido es una de las mayores amenazas a las que puede enfrentar un despacho en esta era de la tecnología, y más aún en la profesión de abogado que se basa

[35] Frase de Thomas Zerdick. https://www.audidat.com/

en la confianza que los clientes depositan en su abogado. Pues una fuga de la información, dañará la imagen del despacho y romperá la confianza de los clientes.

La diligencia profesional en el desempeño del encargo no solo afecta a la formación jurídica, ya sea en el estudio, asesoramiento o ejercicio de acciones en plazos, todo en eras de procurar la mejor solución jurídica posible, sino que también ha de proyectarse en los medios materiales que, como instrumentos o herramientas, constituyen el correcto desarrollo de la actividad profesional. Por ello, se demanda que el despacho haga los esfuerzos necesarios de: Inversión en equipamiento software, actualización de programas y sistemas de seguridad, plan de gestión de riesgos y auditorias de seguridad informática, todo ello con el fin de garantizar un uso seguro de la información, que ya supone, por sí, una obligación general deontológica.

El CDAE dice que: *"El abogado debe actuar siempre honesta y diligentemente, con competencia, con lealtad al cliente, respeto a la parte contraria, guardando secreto de cuanto conociere por razón de su profesión. Y si cualquier Abogado así no lo hiciere, su actuación individual afecta al honor y dignidad de toda la profesión".*[36]

Este deber de diligencia del abogado para con su cliente se contempla en el CDAE: *"Cuando dice que el abogado asesorará y defenderá a su cliente con diligencia, y dedicación, asumiendo personalmente la responsabilidad del trabajo encargado sin perjuicio de las colaboraciones que recabe".*[37]

Por su parte, el EGAE destaca que: *"El abogado está obligado con la parte por él defendida, además de las que se deriven de sus obligaciones contractuales, a cumplir con la misión de defensa que se le encomienda con el máximo celo y diligencia, y guardando el secreto profesional. Para ello, el abogado realizará diligentemente las actividades profesionales que le imponga la defensa del asunto encomendando, ateniéndose a las exigencias técnicas, deontológicas y éticas adecuadas a la tutela jurídica del asunto en cuestión".*[38]

Por ello, es esencial que los despachos profesionales implanten medidas de seguridad y protocolos de actuación que permitan la protección de la información que tratan y custodian, medidas que han de ser de carácter preventivo y reactivo; y que deben permitir minorar, por un lado, el riesgo de fuga o

[36] Preámbulo del CDAE
[37] Artículo 13.10 CDAE
[38] Artículo 42. 1 y 2 EGAE

filtración de información y, por otro, permitir la detección y reacción a tiempo ante un ataque, minorando los daños que este pueda producir.

La ciberseguridad de la información ha pasado a ser una cuestión de prioridad absoluta, por lo que es necesario la concienciación de todos los miembros del despacho ya sea, desde al abogado junior que comienza hasta el socio más veterano. Y es que cualquier incidente puede afectar gravemente a los datos de los clientes del despacho, proveedores u otros compañeros de profesión.

En el caso de que la fuga de información lleve aparejada la de datos personales, el responsable de tratamiento tiene la obligación de notificar a la autoridad de control. Esta notificación se debe realizar sin dilación alguna, desde que se tenga conocimiento por el responsable de tratamiento de que se ha producido una violación de la seguridad de los datos personales. A más tardar 72 horas después de que haya tenido constancia de ella y, en caso de que no sea posible, debe informar de los motivos de la dilación.[39]

La mera sospecha de que ha existido una quiebra no debe dar lugar, todavía a notificación, dado que aún no es posible determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados. Distinto es el caso en el que la quiebra pueda tener un gran impacto, en este caso sería recomendable contactar con la autoridad de supervisión tan rápido como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Además, en el caso, el despacho debe comunicar de forma clara y sencilla al interesado, sin dilación indebida, de la violación de la seguridad de los datos; a fin de que pueda tomar las acciones oportunas de seguridad propia (por ejemplo, cambio de contraseñas o vigilancia de sus correos). Está obligación cesa en caso que el responsable pueda demostrar la improbabilidad de que la violación entrañe un riesgo para derechos y libertades de las personas físicas afectadas. Tal es el supuesto, normalmente, de información cifrada, que la hace inteligible.

Asimismo, no será exigible cuando suponga un *"esfuerzo desproporcionado"*, [40] pudiendo optar en su lugar por una comunicación pública o de otro orden, con tal que se informe efectivamente a los interesados.

[39] Artículo 33 RGPD y Disposición Adicional novena LOPD
[40] Artículo 34 RGPD

El origen de estas fugas de información puede ser tanto interno como externo:

a) Interno: La mayor parte por culpa de los empleados de manera involuntaria (ignorancia, desconocimiento de las herramientas informáticas), por negligencia o error; o por facilitación voluntaria dolosa.

b) Externo: Amenazas que provienen de fuera del despacho y que podemos destacar las siguientes: 1) Hackitivismo: terceros que están en contra el despacho, por razón de determinada clientela, 2) La represalias y venganzas, por clientes descontentos como de personal interno ya fuera de la organización, 3) La sustracción de información confidencial de los clientes, con el fin de buscar una ventaja competitiva de cualquier tipo, 4) Ataques de terceros que solo pretenden un perjuicio en la reputación del despacho, mostrando ante todos los servicios de poca fiabilidad del despacho, 5) Supuestos de actividades propias de competencia desleal.

En la mayoría de los casos, las fugas de información se deben a la ausencia o insuficiencia de medidas de seguridad, producidas por[41]:

a) Causas organizativas: Falta de clasificación de la información, falta de delimitación de quién debe conocerla, falta de formación como causante de errores, Inexistencia de protocolos de seguridad o la inexistencia de acuerdos de confidencialidad en los miembros de la plantilla bien mediante cláusulas especificas o la adhesión a la política general de privacidad y seguridad aplicable al despacho.

b) Causas técnicas: Como pueden ser códigos maliciosos o troyanos (malware), mala formación o uso de las contraseñas para acceso a la nube, uso de los dispositivos móviles como útil para el trabajo.

En el caso de que el daño por la fuga de la información ya este hecho, debemos intentar minimizar el daño con una rápida actuación por nuestra parte. Por eso hay que implantar medidas adecuadas para gestionar y minimizar el impacto del incidente, una vez que este se haya producido. "*Por lo que para ello será necesario realizar una auditoria interna para averiguar qué datos han sido afectados y si la información proviene de los propios archivos del despacho; o bien si afecta a archivos de clientes. Tras la auditoría interna, debe determinarse una auditoría externa para verificar el alcance de la información fugada fuera del despacho".*[42]

[41] Guía gestión de fuga de información pág. 11-14. Se puede acceder a través del siguiente enlace: https://www.aepd.es/media/guias/guia-incibe-aepd-gestionar-fuga-de-informacion.pdf
[42] Ídem pág. 22- 24

En definitiva, de producirse una fuga resulta obligada, en términos de diligencia debida, acometer una auditoría interna y otra externa con el fin de conocer y verificar la gravedad y la eventual difusión o filtración de información al exterior.

4.7 OTRAS CUESTIONES RELEVANTES SOBRE PROTECCIÓN DE DATOS PARA UN DESPACHO DE ABOGADOS

Páginas web y uso de cookies

Es una práctica habitual que los despachos de abogados sean titulares de una página web o blogs de acceso a todo el público que quiera ver y contratar sus servicios jurídicos haciendo uso de estas herramientas. En estos casos, además de cumplir con la normativa de protección de datos, están obligados a cumplir con lo establecido en la Ley 34/2003, de Servicios de la Sociedad de la Información (en adelante LSSI).

Todo despacho profesional tiene que ser cuidadoso respecto a la información que pública en su web o blog, debiendo tener siempre presente: el secreto profesional y la normativa reguladora del derecho a la protección de datos. Para que no sea sancionado como en el siguiente caso, la AEPD sanciono a una procuradora, titular de un blog, por publicar la fotografía de la denunciante junto con un documento judicial relacionado con la violencia de género.[43]

También es importante destacar los procedimientos de recogida de datos a través de la web del despacho, ya sean formularios habilitados para contactar o consultar, respecto de los que se debe cumplir el deber de informar en la recogida de los datos y de obtener el consentimiento para su tratamiento. *"La información que se proporcione a nuestros clientes deberá ser en un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso".*[44]

En lo que respecta a las comunicaciones comerciales electrónicas se prohíbe el envío de estas, cuando no hubieran sido solicitadas o expresamente autorizadas por los destinatarios. En el caso de que tenga la autorización para su envío, el despacho debe ofrecer al cliente/destinatario de la comunicación la posibilidad oponerse al tratamiento de sus datos, de una manera sencilla incluyendo una dirección de correo electrónica válida para que pueda ejercitar este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

[43] AEPD proc PS/000446/2011. Disponible en el siguiente enlace: https://www.aepd.es/resoluciones/
[44] https://ayudaleyprotecciondatos.es/2018/11/12/derecho-informacion-rgpd/

Los despachos de abogados como prestadores de servicios de la sociedad de la información a través de sus webs, también pueden hacer uso de dispositivos de almacenamiento y recuperación de datos como identificadores de sesión "cookies" en equipos terminales de los destinatarios, pero solo si estos han dado su consentimiento después de que se les haya informado de manera clara y completa sobre los fines de tratamiento de los datos. Para que la política de cookies del despacho sea de acuerdo al RGPD debe cumplir con los siguientes requisitos: a) Debe ser transparente; b) Debe obtenerse el consentimiento previo solicitado a través de una acción afirmativa y c) Debe otorgarse la posibilidad de retirar el consentimiento en cualquier momento.[45]

Utilización del "cloud computing"

Los servicios en la nube o "cloud computing" son cada vez más utilizados porque permiten una considerable reducción de costes y mejorar de manera más eficaz la gestión de la información en un despacho sin necesidad de disponer de servidores o de software en el propio despacho.

Esto permite al despacho acceder a una serie de servicios, como puede ser almacenamiento de documentos, gestión del despacho, contabilidad, base de datos de jurisprudencia o legislación, o de compartición de documentación e información con clientes o con otros despachos.

El cumplimiento de la legislación de protección de datos es un aspecto esencial a la hora de contratar servicios en la nube por parte de un despacho de abogados. Los despachos que contraten servicios de cloud computing son los responsables pues a ellos les corresponde la decisión sobre la finalidad, el contenido y el uso del tratamiento, así como la decisión sobre optar por los servicios en la nube.

Este servicio ha llegado a ser tan utilizado por los despachos de abogados que se ha elaborado un "Informe de la AEPD y el Consejo General de la Abogacía sobre la utilización del cloud computing" por los despachos de abogados y el derecho a la protección de datos de carácter personal en materia de seguridad y confidencialidad, comentando los aspectos esenciales a tener en cuenta durante la selección del proveedor de servicios en la nube.[46]

Comunicación abogado-cliente y mensajería instantánea

[45] https://www.cookiebot.com/es/rgpd-cookies/
[46] https://www.abogacia.es/wp-content/uploads/2012/07/informe_CLOUDCOMPUTING.pdf

El uso del Whatsapp, Telegram, Skype, Facebook o Messenger ha llegado a los clientes de los despachos y de los abogados y a sus relaciones con estos, produciendo un tratamiento de datos personales y entrando en juego, la normativa sobre protección de datos.

Aunque, lo malo de estas aplicaciones es que raramente se garantiza la seguridad de la información transmitida, por lo que no es recomendable el uso de las mismas en el tratamiento de datos de carácter personal en el ejercicio de profesiones de tan alta importancia como la labor del abogado, sometidas al deber de secreto profesional y a la normativa RGPD y LOPD.

Por lo que cabe destacar en esta materia, el "Dictamen de la Autoridad Catalana de Protección de Datos" (ACPD), el CNS-24/2013, en el que abordó una consulta de un Colegio de Abogados, en relación con el uso de la aplicación Whatsapp en el ámbito profesional de las relaciones entre abogado y cliente[47]. Se entiende que, sin perjuicio de la eventual responsabilidad legal que pudiera corresponder a la citada aplicación por el inadecuado tratamiento de los datos de sus usuarios, el abogado tiene un grado de responsabilidad específico respecto al tratamiento de los datos de sus propios clientes, entre lo que se incluye la elección del canal de comunicación más adecuado para tales fines.

Whatsapp reconoce en su <<política de privacidad>>, accesible en su sitio web, que no puede garantizar la seguridad de la información transmitida. Concluye la ACPD que "teniendo en cuenta esto, junto con varias vulnerabilidades detectadas, y dado que en el contexto de la relación entre abogado y clientes puede ser habitual la comunicación y tratamiento de datos sensibles la utilización de Whatsapp no resulta recomendable, en relación con la seguridad exigida" por la normativa aplicable.[48]

Tratamiento de datos derivados de la Ley de Blanqueo de Capitales

La Ley 10/2010, de Prevención del Blanqueo de Capitales vino a afectar al ejercicio de las profesiones jurídicas en general, y al ejercicio de la abogacía en particular. Impone al abogado la obligación de diligencia debida en esta materia, lo que: implica la identificación formal de aquellas personas con las que se establezca una relación negocial o intervengan en operaciones, y, además, exige la identificación del titular real.

[47] http://www.aspectosprofesionales.info/2013/07/uso-de-whatsapp-en-el-ambito.html
[48] Ídem

El art.2 de esta ley establece los supuestos en los que está pensado el deber de colaboración del abogado, abarcando desde actuaciones para los clientes encaminados a la gestión hasta actuaciones por cuenta del cliente en operaciones financieras.[49]

Por lo tanto, ante cualquier hecho calificado como de sospechoso, o incluso se detecte una "mera tentativa" de hecho u de operación, debe denunciarse ante el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac). Teniendo esta comunicación amparo en el Art. 6.1 c) RGPD.

Cuestión distinta es cuando el abogado actúa o va actuar judicialmente en un proceso en defensa de los intereses de un cliente, ya que el deber de colaboración solo está pensado para los supuestos de asesoramiento en la gestión, prevaleciendo el derecho de defensa y el secreto profesional cuando el papel del letrado se ciñe al asesoramiento estrictamente jurídico dentro del ejercicio de defensa, ya que lo contrario rompería la confianza entre abogado-cliente.

Publicación de datos de colegiados abogados por los colegios profesionales

Los datos de contacto e identificativos de los abogados son también objeto de amparo por las normas de protección de datos, cuando son publicados por mandato de la ley y sin su consentimiento, por los colegios profesionales y sus consejos generales.

Esto responde a una potestad de ordenación profesional que las leyes han atribuido a las corporaciones de derecho público, ya que resultado de obligado cumplimiento para estas, el tener actualizado el registro de colegiados en la ventanilla única de su web, con la finalidad de protección de los intereses de los ciudadanos y clientes.

4.8 RIESGOS DE NO CUMPLIR CON LA NORMATIVA (RÉGIMEN SANCIONADOR)

El abogado o despacho de abogados debe cumplir con la normativa RGPD, tanto cuando actúa como responsable o encargado de tratamiento ya que puede ser sancionado con cuantías muy elevadas. Y es que para evitar que se produzca una lesión en el tratamiento de los datos de un cliente, una de las grandes novedades del RGPD es el aumento de las sanciones económicas llegando en algunos casos hasta 20.000.000 euros o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo

[49] Artículo 2 Ley de Blanqueo de Capitales

del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.[50]

Estas multas administrativas pueden ser muy graves, graves y leves y se gradúan en función de que se den distintas circunstancias como pueden ser: *"1) La naturaleza, gravedad y duración de la infracción, 2) la intencionalidad o negligencia en la infracción (...) 11) Cualquier otro factor agravante o atenuante"*[51]. Por ello es importante anticiparse instaurando correcciones ante posibles peligros o incumplimientos del RGPD. Ya que con ello se puede reducir los daños y a la vez mostrar voluntad por cumplir con la normativa de protección de datos lo que tendrá su virtualidad en la graduación de la eventual sanción.

Respecto a la figura del DPD no tiene responsabilidad administrativa, pero sí que puede tener responsabilidad civil que el responsable, en este caso el despacho le pueda exigir por el desempeño de su labor.

En cuanto al régimen sancionador se puede iniciar de oficio, por la AEPD, o a instancia de parte, previa reclamación, y siempre que esta haya sido admitida a trámite. Resaltar que, si el responsable o encargado del tratamiento del despacho hubiere adoptado medidas correctivas tras una advertencia por parte de la AEPD de eventual irregularidad, tal autoridad puede no incoar expediente, siempre que no se haya causado perjuicios y que las medidas sean efectivas en la protección del derecho del afectado.

5. TRATAMIENTO DE DATOS Y CONSENTIMIENTO DE MENORES

En materia de protección de datos, los menores de edad tienen una especial protección, pues pese a haber nacido en la era de la tecnología son considerados vulnerables pues no están suficientemente maduros para conocer los riesgos y amenazas que trae consigo que cualquier tercero pueda tener o acceder a sus datos. En definitiva, esa falta de madurez hace que su protección sea uno de los objetivos fundamentales que tratan de reforzar su protección tanto el RGPD y LOPD.

Es importante para la labor del abogado saber cuándo trata datos de un menor si necesita de la autorización de sus padres o tutores para consentir el tratamiento de sus datos. En este caso la nueva LOPD reduce de los 14 a los 13 años de edad, en la que un menor de edad pueda dar su consentimiento para el tratamiento de sus datos.

[50] Artículo 83.3 RGPD
[51] Artículo 83.2 RGPD

En el caso de que se recaben sus datos sin su consentimiento, cuando el menor esté en condiciones de prestarlo o el del titular de su patria potestad o tutela cuando el menor carezca de capacidad para ello, sin que el abogado haya realizado esfuerzos razonables para verificar la validez del consentimiento prestado por el menor o por el titular de su patria potestad o tutela, puede suponer la calificación de infracción grave con su correspondiente sanción para el despacho.[52]

Respecto al menor como titular del derecho a la protección de datos personales, puede a su vez ejercitar los derechos que este conlleva. Son derechos personalísimos cuyo ejercicio únicamente cabe por el interesado. No obstante, podrá actuar el representante legal del menor cuando se encuentre en situación de incapacidad o minoría de edad que imposibilite el ejercicio personal de los derechos. El RGPD no dice nada respecto a cuándo el menor de edad es capaz para prestar su consentimiento ante tales derechos y cuando no lo es. Haciendo una trasposición al momento actual de lo dicho por Rebollo Delgado y Serrano Pérez: *"Podemos entender que en los supuestos en que no se precise el consentimiento de los titulares de la patria potestad o tutela podrá ejercitarse por el menor entre 13 a 18 años, los derechos correspondientes a la protección de datos".*[53]

En definitiva, se considera que debe aplicarse la regla objetiva de la edad, tanto para el consentimiento, como para el ejercicio de los derechos que incumben al derecho de protección de datos con la finalidad de conseguir una mayor seguridad jurídica, ya que no tendría sentido establecer edades distintas.

6. CONCLUSIONES

El propósito de este trabajo ha sido el realizar un breve recorrido histórico sobre las primeras señales de vida del derecho a la protección de datos, para entender por qué se está haciendo cada vez más importante en nuestros días y la razón por la que merece una especial protección. Mostrando la importancia y trascendencia que este derecho tenía desde muchas décadas atrás no solo en España sino en otras legislaciones.

El trabajo se ha centrado principalmente en los efectos que tiene en la actualidad, la protección de datos para los abogados o un despacho de abogados. La elección de este tema es debido a su importancia actual y más aún en esta etapa de adaptación por parte de empresas y profesionales del

[52] Artículo 73 RGPD

[53] **REBOLLO DELGADO, L. Y SERRANO PÉREZ, M.M**. Manual de Protección de Datos, Dykinson, Madrid, 2014, págs. 126 y 303

derecho a las nuevas normativas del RGPD y LOPD. Es un área que muchos abogados desconocen y que pienso que debería fomentarse y concienciarse mucho más, incluso desde el grado porque es un área en auge constante debido a todos los avances tecnológicos y que, todo letrado debería tener actualizado.

Porque el uso y navegación en Internet es un campo cada vez más recurrente cuando un letrado quiere obtener información legislativa y jurisprudencial, o como medio de comunicación con las Administraciones Públicas (presentación telemática de escritos, declaraciones, liquidaciones, etc.) o judiciales (LexNet) [54] que exigen que cada vez los abogados estemos más formados no solamente jurídicamente sino también, que tengamos conocimientos sobre protección de datos y un dominio básico de la informática.

Es de fundamental importancia para un despacho estar debidamente actualizado a lo que exige la normativa de protección de datos, pues muchas veces, las causas de fugas de información son debidas a una falta de formación. Por lo que hay que concienciar en materia de ciberseguridad a todos los miembros del despacho para así, evitarnos daños reputacionales o sanciones civiles, penales, administrativas o deontológicas.

Para finalizar, decir que tener conocimientos en materia de protección de datos no solamente es una obligación legal, sino que puede ser una "marca personal" para cualquier despacho no solamente con el fin de evitar unas posibles sanciones. Sino para transmitir a sus clientes la calidad de sus servicios y mantener intacta la confianza de los clientes, pues la confianza abogado-cliente es el pilar fundamental de nuestra profesión y a la vez, es una exigencia de la sociedad que puede determinar o no nuestro éxito profesional.

7. <u>BIBLIOGRAFÍA</u>

- BOBBIO, Norberto, "El tiempo de los derechos", Editorial Sistema, Madrid, España, 1991.

[54] **Jesús Cobos Tubilla, Ignacio De Luis Otero, Pablo Linde Puelles, Emilio Ramírez Matos, María Rius Peña**: Protección de datos. Aplicación del RGPD. Francis Lefebvre 2018. Pág. 95

- JESÚS COBOS TUBILLA, IGNACIO DE LUIS OTERO, PABLO LINDE PUELLES, EMILIO RAMÍREZ MATOS, MARÍA RIUS PEÑA: Protección de datos. Aplicación del RGPD. Francis Lefebvre 2018.
- LUCAS MURILLO, Pablo "El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática", Editorial Tecnos, 1990.
- REBOLLO DELGADO, L. Y SERRANO PÉREZ, M.M. Manual de Protección de Datos, Dykinson, Madrid, 2014.

GUÍAS PRÁCTICAS:

- Guía práctica de Análisis de riesgos. AEPD 2018. Disponible en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf
- Guía práctica de Evaluaciones de impacto. AEPD 2018. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
- Guía Listado de cumplimiento normativo del RGPD. AEPD. Disponible en: https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf
- Guía Modelo cláusula informativa. Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf
- Guía Cómo Gestionar una Fuga de Información en un despacho de abogados. CGAE. E-Book. Guías TIC. Disponible en: https://www.aepd.es/media/guias/guia-incibe-aepd-gestionar-fuga-de-informacion.pdf
- Guía GT29 "Directrices sobre los delegados de protección de datos". Disponible en: https://www.aepd.es/media/criterios/wp243rev01-es.pdf
- Informe 2000-0000 AEPD que trata sobre "Tratamiento por Abogados y Procuradores de los datos de las partes en un proceso". Disponible en: https://ayudaleyprotecciondatos.es/2013/02/07/tratamiento-abogados-datos-parte-contraria/

Jurisprudencia:

- Sentencia del Tribunal Constitucional 254/1993,11/1998, 202/1999,134/1999, 115/2000, 186/2000 y 292/2000
- Audiencia Provincial de Las Palmas 10-06-2013
- Resolución por AEPD PS/000446/2011.

LEGISLACIÓN:

- Constitución Española, de 29 de diciembre de 1978
- Directiva 95/46/CE
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto 658/2011, de 22 de junio, por el que se aprueba el Estatuto General de la Abogacía Española
- Código Deontológico de la Abogacía, de 27 de septiembre de 2002.
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo

Web grafía:

- http://lopdyseguridad.es/a-proposito-de-las-citas-en-exposiciones-de-motivos/
- http//www.congreso.es/public_oficiales/L0/SEN/DS/S_1978_060.PDF
- https://ayudaleyprotecciondatos.es/2013/02/07/tratamiento-abogados-datos-parte-contraria/
- https://protecciondatos-lopd.com/empresas/privacy-by-design/
- https://www.audidat.com/
- https://ayudaleyprotecciondatos.es/2018/11/12/derecho-informacion-rgpd/
- https://www.abogacia.es/wp-content/uploads/2012/07/informe_CLOUDCOMPUTING.pdf
- http://www.aspectosprofesionales.info/2013/07/uso-de-whatsapp-en-el-ambito.html